

RPKI Engine

1.0

Generated by Doxygen 1.5.5

Thu Jun 12 22:02:16 2008

Contents

1	RPKI Engine Reference Manual	1
2	Installation Guide	1
3	Operation Guide	3
4	Left-right protocol	16
5	Publication protocol	26
6	Namespace Documentation	30
7	Class Documentation	67
8	File Documentation	473

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](#).

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

- The [installation instructions](#)
- The [operation instructions](#)
- A description of the [left-right protocol](#)
- A description of the [publication protocol](#)

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](#)

2 Installation Guide

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

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

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

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

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

Before attempting to build the package, 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.

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

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

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

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

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

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

At this point, you should have all the necessary software installed. You will probably want to test it. All tests should be run from the `rpkid/` directory.

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 Guide

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

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

Warning:

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

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

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

- [rpkid.py](#): The main RPKI engine daemon.
- [pubd.py](#): The [publication](#) engine daemon.
- [rootd.py](#): A separate daemon for handling the root of an RPKI certificate tree. This is essentially a stripped down version of [rpkid](#) with no SQL database, no left-right protocol implementation, and only the parent side of the up-down protocol. It's separate because the root is a special case in several ways and it was simpler to keep the special cases out of the main daemon.

- `irdbd.py`: A sample implementation of an IR database daemon. `rpkid` calls into this to perform lookups via the left-right protocol.
- `irbe-cli.py`: A command-line client for the left-right control protocol.
- `cross-certify.py`: A BPKI cross-certification tool.
- `irbe-setup.py`: An example of a script to set up the mappings between the IRDB and `rpkid`'s own database, using the left-right control protocol.
- `cronjob.py`: A trivial HTTP client used to drive `rpkid` cron events.
- `testbed.py`: A test tool for running a collection of `rpkid` and `irdb` instances under common control, driven by a unified test script.
- `testpoke.py`: A simple client for the up-down protocol, mostly compatible with APNIC's `rpki_poke.pl` tool.

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

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

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

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

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

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

3.1 rpkiid.py

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

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

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

Config file options:

- `startup-message`: String to log on startup, useful when debugging a collection of [rpkiid](#) instances at once.
- `sql-username`: Username to hand to MySQL when connecting to [rpkiid](#)'s database.
- `sql-database`: MySQL's database name for [rpkiid](#)'s database.
- `sql-password`: Password to hand to MySQL when connecting to [rpkiid](#)'s database.
- `bpki-ta`: Name of file containing BPKI trust anchor. All BPKI certificate verification within [rpkiid](#) traces back to this trust anchor.
- `rpkiid-cert`: Name of file containing [rpkiid](#)'s own BPKI EE certificate.
- `rpkiid-key`: Name of file containing RSA key corresponding to [rpkiid-cert](#).
- `irbe-cert`: Name of file containing BPKI certificate used by IRBE when talking to [rpkiid](#).
- `irdb-cert`: Name of file containing BPKI certificate used by [irdbd](#).
- `irdb-url`: Service URL for [irdbd](#). Must be a `https://` URL.
- `server-host`: Hostname or IP address on which to listen for HTTPS connections. Current default is `INADDR_ANY` (IPv4 0.0.0.0); this will need to be hacked to support IPv6 for production.
- `server-port`: TCP port on which to listen for HTTPS connections.

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`]". Certificates, keys, and trust anchors may be either DER or PEM format.

Config file options:

- `sql-username`: Username to hand to MySQL when connecting to `pubd`'s database.
- `sql-database`: MySQL's database name for `pubd`'s database.
- `sql-password`: Password to hand to MySQL when connecting to `pubd`'s database.
- `bpki-ta`: Name of file containing master BPKI trust anchor for `pubd`. All BPKI validation in `pubd` traces back to this trust anchor.
- `irbe-cert`: Name of file containing BPKI certificate used by IRBE when talking to `pubd`.
- `pubd-cert`: Name of file containing BPKI certificate used by `pubd`.

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

3.3 rootd.py

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

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

Config file options:

- `bpki-ta`: Name of file containing BPKI trust anchor. All BPKI certificate validation in `rootd` traces back to this trust anchor.
- `rootd-bpki-cert`: Name of file containing `rootd`'s own BPKI certificate.
- `rootd-bpki-key`: Name of file containing RSA key corresponding to `rootd-bpki-cert`.
- `rootd-bpki-crl`: Name of file containing BPKI CRL that would cover `rootd-bpki-cert` had it been revoked.
- `child-bpki-cert`: Name of file containing BPKI certificate for `rootd`'s one and only child (RPKI engine to which `rootd` issues an RPKI certificate).
- `server-host`: Hostname or IP address on which to listen for HTTPS connections. Default is `localhost`.
- `server-port`: TCP port on which to listen for HTTPS connections.

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

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

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

Config file options:

- `startup-message`: String to log on startup, useful when debugging a collection of `irdbd` instances at once.
- `sql-username`: Username to hand to MySQL when connecting to `irdbd`'s database.
- `sql-database`: MySQL's database name for `irdbd`'s database.
- `sql-password`: Password to hand to MySQL when connecting to `irdbd`'s database.
- `bpki-ta`: Name of file containing BPKI trust anchor. All BPKI certificate validation in `irdbd` traces back to this trust anchor.

- `irdbd-cert`: Name of file containing irdbd's own BPKI certificate.
- `irdbd-key`: Name of file containing RSA key corresponding to `irdbd-cert`.
- `rpkid-cert`: Name of file containing certificate used the one and only by [rpkid](#) instance authorized to contact this [irdbd](#) instance.
- `https-url`: Service URL for [irdbd](#). Must be a `https://` URL.

3.5 irbe-cli.py

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

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

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

```
$Id: irbe-cli.py 1880 2008-06-12 21:54:53Z 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.
```

```
Usage:
```

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

```

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

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

```

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

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

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

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

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

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

Config file options:

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

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

3.6 cross-certify.py

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

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

3.7 irbe-setup.py config file

Warning:

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

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

Options in the `"[irbe-cli]"` section:

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

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

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

3.8 cronjob.py

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

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

Config file options:

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

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

3.9 testbed.py:

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

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

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

`testbed.conf` options:

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

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

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

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

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

Operators in subsequent (update) documents:

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

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

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

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

3.10 testpoke.py

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

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

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

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

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

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

Sample configuration file:

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

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



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

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

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

requests:
  list:
    type: list
    issue:
      type: issue
      class: 1
      sia: [ "rsync://bandicoot.invalid/some/where/" ]
      revoke:
        type: revoke
        class: 1
      ski: "CB5K6APY-4KcGAW9jaK_cVPXX0"
```

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

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

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

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

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

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 certificate a new one should be generated, measured in seconds. At present this only affects the one-off EE certificates associated with ROAs.
- `bpki_cert` (element): BPKI CA certificate for this `<self/>`. This is used as part of the certificate chain when validating incoming TLS and CMS messages, and should be the issuer of cross-certification BPKI certificates used in `<repository/>`, `<parent/>`, and `<child/>` objects. If the `bpki_glue` certificate is in use (below), the `bpki_cert` certificate should be issued by the `bpki_glue` certificate; otherwise, the `bpki_cert` certificate should be issued by the per-engine `bpki_ta` certificate.
- `bpki_glue` (element): Another BPKI CA certificate for this `<self/>`, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the `bpki_glue` certificate should be the issuer of the `bpki_cert` certificate and should be issued by the per-engine `bpki_ta` certificate; if not needed, the `bpki_glue` certificate should be left unset.

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

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

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

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

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

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

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

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 capability 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 an IRBE to use to configure a publication engine, the second is the interface by which authorized clients request publication of specific objects.

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

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

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. 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 the

object to be published or withdrawn has a "uri" attribute which contains the publication URI. For "publish" actions, the XML element body contains the DER object to be published, encoded in Base64; for "withdraw" actions, the XML element body is empty.

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

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 in both the control and [publication](#) subprotocols.

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

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

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

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 cross

-certify

6.1.1 Detailed Description

-certify

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

Much of this code lifted from `rpki.x509.X509.issue()`, but this is a sufficiently different purpose that it's probably not worth refactoring.

```
Usage: python cross-certify.py { -i | --in      } input_cert
                                { -c | --ca      } issuing_cert
                                { -k | --key     } issuing_cert_key
                                { -s | --serial  } serial_filename
                                [ { -h | --help } ]
                                [ { -o | --out   } filename (default: stdout) ]
                                [ { -l | --lifetime } timedelta (default: 30 days) ]
```

```
$Id: cross-certify.py 1880 2008-06-12 21:54:53Z 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.

6.2 Package cross-certify

Functions

- def `usage`

Variables

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

6.2.1 Function Documentation

6.2.1.1 def `cross-certify.usage` (*code*)

Definition at line 42 of file `cross-certify.py`.

6.2.2 Variable Documentation

6.2.2.1 tuple `cross-certify.cert` = `rpki.x509.X509(POWpkix = x)`

Definition at line 96 of file `cross-certify.py`.

6.2.2.2 tuple `cross-certify.child` = `rpki.x509.X509(Auto_file = a)`

Definition at line 55 of file `cross-certify.py`.

6.2.2.3 tuple cross-certify::f = open(serial_file, "r")

Definition at line 73 of file cross-certify.py.

6.2.2.4 tuple cross-certify.keypair = rpki.x509.RSA(Auto_file = a)

Definition at line 61 of file cross-certify.py.

6.2.2.5 tuple cross-certify::lifetime = rpki.sundial.timedelta(days = 30)

Definition at line 47 of file cross-certify.py.

6.2.2.6 cross-certify.notAfter = now+lifetime

Definition at line 70 of file cross-certify.py.

6.2.2.7 tuple cross-certify.now = rpki.sundial.now()

Definition at line 69 of file cross-certify.py.

6.2.2.8 cross-certify.output = None

Definition at line 46 of file cross-certify.py.

6.2.2.9 tuple cross-certify.parent = rpki.x509.X509(Auto_file = a)

Definition at line 59 of file cross-certify.py.

6.2.2.10 int cross-certify::serial = f.read()

Definition at line 74 of file cross-certify.py.

6.2.2.11 cross-certify.serial_file = a

Definition at line 63 of file cross-certify.py.

6.2.2.12 tuple cross-certify.x = POW.pkix.Certificate()

Definition at line 80 of file cross-certify.py.

6.3 Package irbe

-cli

6.3.1 Detailed Description

-cli

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

\$Id: irbe-cli.py 1880 2008-06-12 21:54:53Z 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 irbe-cli

Classes

- class [bsc_elt](#)
- class [certificate_elt](#)
- class [child_elt](#)
- class [client_elt](#)
- class [cmd_elt_mixin](#)
- class [cmd_msg_mixin](#)
- class [config_elt](#)
- class [crl_elt](#)
- class [left_right_cms_msg](#)
- class [left_right_msg](#)
- class [left_right_sax_handler](#)
- class [manifest_elt](#)
- class [parent_elt](#)
- class [publication_cms_msg](#)
- class [publication_msg](#)
- class [publication_sax_handler](#)
- class [repository_elt](#)
- class [roa_elt](#)
- class [route_origin_elt](#)
- class [self_elt](#)
- class [UsageWrapper](#)

Functions

- def `call_daemon`
- def `usage`

Variables

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

6.4.1 Function Documentation

6.4.1.1 `def irbe-cli.call_daemon (cms_class, client_key, client_cert, server_ta, url, q_msg)`

Definition at line 223 of file `irbe-cli.py`.

6.4.1.2 `def irbe-cli.usage (code = 1)`

Definition at line 206 of file `irbe-cli.py`.

6.4.2 Variable Documentation

6.4.2.1 `tuple irbe-cli::argv = sys.argv[1:]`

Definition at line 241 of file `irbe-cli.py`.

6.4.2.2 `tuple irbe-cli.cfg = rpki.config.parser(cfg_file, "irbe-cli")`

Definition at line 263 of file `irbe-cli.py`.

6.4.2.3 irbe-cli.cfg_file = "irbe.conf"

Definition at line 246 of file irbe-cli.py.

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

Definition at line 287 of file irbe-cli.py.

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

Definition at line 286 of file irbe-cli.py.

6.4.2.6 irbe-cli.cms_class = left_right cms_msg,

Definition at line 285 of file irbe-cli.py.

6.4.2.7 irbe-cli.pem_out = None

Definition at line 24 of file irbe-cli.py.

6.4.2.8 irbe-cli.q_msg = q_msg_left_right

Definition at line 274 of file irbe-cli.py.

6.4.2.9 tuple irbe-cli.q_msg_left_right = left_right_msg()

Definition at line 265 of file irbe-cli.py.

6.4.2.10 tuple irbe-cli.q_msg_publication = publication_msg()

Definition at line 268 of file irbe-cli.py.

6.4.2.11 list irbe-cli::q_pdu = left_right_msg.pdus[argv[0]]

Definition at line 273 of file irbe-cli.py.

6.4.2.12 tuple irbe-cli::server_ta

Initial value:

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

Definition at line 288 of file irbe-cli.py.

6.4.2.13 `list irbe-cli.top_opts = ["config=", "help", "pem_out=", "verbose"]`

Definition at line 204 of file irbe-cli.py.

6.4.2.14 `tuple irbe-cli::url = cfg.get("rpkid-url")`

Definition at line 290 of file irbe-cli.py.

6.4.2.15 `tuple irbe-cli.usage_fill = UsageWrapper(subsequent_indent = " " * 4)`

Definition at line 33 of file irbe-cli.py.

6.4.2.16 `irbe-cli.verbose = False`

Definition at line 247 of file irbe-cli.py.

6.5 Package irdbd

Functions

- def [handler](#)

Variables

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

6.5.1 Detailed Description

IR database daemon.

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

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

\$Id: irdbd.py 1880 2008-06-12 21:54:53Z 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 irdbd.handler (query, path)`

Definition at line 30 of file irdbd.py.

6.5.3 Variable Documentation

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

Definition at line 114 of file irdbd.py.

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

Definition at line 102 of file irdbd.py.

6.5.3.3 `irdbd.cfg_file = "irdbd.conf"`

Definition at line 90 of file irdbd.py.

6.5.3.4 `tuple irdbd.client_ta = (bpki_ta, rpki_cert)`

Definition at line 130 of file irdbd.py.

6.5.3.5 tuple irdbd.cur = db.cursor()

Definition at line 112 of file irdbd.py.

6.5.3.6 tuple irdbd.db

Initial value:

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

Definition at line 108 of file irdbd.py.

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

Definition at line 133 of file irdbd.py.

6.5.3.8 string irdbd.host = "localhost"

Definition at line 131 of file irdbd.py.

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

Definition at line 116 of file irdbd.py.

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

Definition at line 117 of file irdbd.py.

6.5.3.11 int irdbd.port = 443

Definition at line 132 of file irdbd.py.

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

Definition at line 115 of file irdbd.py.

6.5.3.13 irdbd.server_cert = irdbd_cert,

Definition at line 129 of file irdbd.py.

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

Definition at line 104 of file `irdbd.py`.

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

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

6.6 Package pubd**Classes**

- class `pubd_context`

Functions

- def `main`

Variables

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

6.6.1 Detailed Description

RPKI publication engine.

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

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

```
$Id: pubd.py 1880 2008-06-12 21:54:53Z 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.

6.6.2 Function Documentation

6.6.2.1 `def pubd.main ()`

Definition at line 127 of file `pubd.py`.

6.6.3 Variable Documentation

6.6.3.1 `pubd.cfg_file = "pubd.conf"`

Definition at line 112 of file `pubd.py`.

6.6.3.2 `pubd.profile = False`

Definition at line 113 of file `pubd.py`.

6.7 Package rootd

Classes

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

Functions

- def `compose_response`
- def `del_subject_cert`
- def `get_subject_cert`
- def `set_subject_cert`
- def `stash_subject_pkcs10`
- def `up_down_handler`

Variables

- tuple `bpki_ta` = `rpki.x509.X509`(Auto_file = `cfg.get("bpki-ta")`)
- tuple `cfg` = `rpki.config.parser`(`cfg_file`, "rootd")
- string `cfg_file` = "rootd.conf"
- tuple `child_bpki_cert` = `rpki.x509.X509`(Auto_file = `cfg.get("child-bpki-cert")`)
- tuple `client_ta` = (`bpki_ta`, `child_bpki_cert`)

- `handlers = up_down_handler)`
- `host = https_server_host,`
- `tuple https_server_host = cfg.get("server-host", "")`
- `tuple https_server_port = int(cfg.get("server-port"))`
- `port = https_server_port,`
- `tuple rootd_base = cfg.get("rootd_base", "rsync://" + rootd_name + ".invalid/")`
- `tuple rootd_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("rootd-bpki-cert"))`
- `tuple rootd_bpki_crl = rpki.x509.CRL(Auto_file = cfg.get("rootd-bpki-crl"))`
- `tuple rootd_bpki_key = rpki.x509.RSA(Auto_file = cfg.get("rootd-bpki-key"))`
- `tuple rootd_cert = cfg.get("rootd_cert", rootd_base + "rootd.cer")`
- `tuple rootd_name = cfg.get("rootd_name", "wombat")`
- `tuple rpki_issuer = rpki.x509.X509(Auto_file = cfg.get("rpki-issuer"))`
- `tuple rpki_key = rpki.x509.RSA(Auto_file = cfg.get("rpki-key"))`
- `tuple rpki_pkcs10_filename = cfg.get("rpki-pkcs10-filename", "")`
- `tuple rpki_subject_filename = cfg.get("rpki-subject-filename")`
- `tuple rpki_subject_lifetime = rpki.sundial.timedelta(days = 30)`
- `server_cert = rootd_bpki_cert,`

6.7.1 Detailed Description

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

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

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

```
$Id: rootd.py 1880 2008-06-12 21:54:53Z 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 Function Documentation

6.7.2.1 `def rootd.compose_response (r_msg)`

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

6.7.2.2 def rootd.del_subject_cert ()

Definition at line 46 of file rootd.py.

6.7.2.3 def rootd.get_subject_cert ()

Definition at line 34 of file rootd.py.

6.7.2.4 def rootd.set_subject_cert (cert)

Definition at line 41 of file rootd.py.

6.7.2.5 def rootd.stash_subject_pkcs10 (pkcs10)

Definition at line 49 of file rootd.py.

6.7.2.6 def rootd.up_down_handler (query, path)

Definition at line 133 of file rootd.py.

6.7.3 Variable Documentation**6.7.3.1 tuple rootd.bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))**

Definition at line 172 of file rootd.py.

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

Definition at line 170 of file rootd.py.

6.7.3.3 rootd.cfg_file = "rootd.conf"

Definition at line 158 of file rootd.py.

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

Definition at line 176 of file rootd.py.

6.7.3.5 tuple rootd.client_ta = (bpki_ta, child_bpki_cert)

Definition at line 193 of file rootd.py.

6.7.3.6 rootd.handlers = up_down_handler)

Definition at line 196 of file rootd.py.

6.7.3.7 rootd.host = https_server_host,

Definition at line 194 of file rootd.py.

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

Definition at line 178 of file rootd.py.

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

Definition at line 179 of file rootd.py.

6.7.3.10 rootd.port = https_server_port,

Definition at line 195 of file rootd.py.

6.7.3.11 tuple rootd.rootd_base = cfg.get("rootd_base", "rsync://" + rootd_name + ".invalid/")

Definition at line 188 of file rootd.py.

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

Definition at line 174 of file rootd.py.

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

Definition at line 175 of file rootd.py.

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

Definition at line 173 of file rootd.py.

6.7.3.15 tuple rootd.rootd_cert = cfg.get("rootd_cert", rootd_base + "rootd.cer")

Definition at line 189 of file rootd.py.

6.7.3.16 `tuple rootd.rootd_name = cfg.get("rootd_name", "wombat")`

Definition at line 187 of file rootd.py.

6.7.3.17 `tuple rootd.rpki_issuer = rpki.x509.X509(Auto_file = cfg.get("rpki-issuer"))`

Definition at line 182 of file rootd.py.

6.7.3.18 `tuple rootd.rpki_key = rpki.x509.RSA(Auto_file = cfg.get("rpki-key"))`

Definition at line 181 of file rootd.py.

6.7.3.19 `tuple rootd.rpki_pkcs10_filename = cfg.get("rpki-pkcs10-filename", "")`

Definition at line 185 of file rootd.py.

6.7.3.20 `tuple rootd.rpki_subject_filename = cfg.get("rpki-subject-filename")`

Definition at line 184 of file rootd.py.

6.7.3.21 `tuple rootd.rpki_subject_lifetime = rpki.sundial.timedelta(days = 30)`

Definition at line 32 of file rootd.py.

6.7.3.22 `rootd.server_cert = rootd_bpki_cert,`

Definition at line 192 of file rootd.py.

6.8 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](#)

6.9 Package rpki.config

Classes

- class [parser](#)

6.9.1 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.

6.10 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 [DBConsistencyError](#)
- 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](#)

6.10.1 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.

6.11 Package rpki.https

Classes

- class [Checker](#)
- class [httpsClient](#)
- class [httpsServer](#)
- class [requestHandler](#)

Functions

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

Variables

- [debug_tls_certs](#) = False
- [disable_tls_certificate_validation_exceptions](#) = False
- string [rpki_content_type](#) = "application/x-rpki"

6.11.1 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.

6.11.2 Function Documentation

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

Build a dynamic TLS trust anchor cache.

Definition at line 45 of file https.py.

6.11.2.2 `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.

6.11.2.3 `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.

6.11.2.4 `def rpki.https.tlsite_certChain (x509)`

Utility function to construct tlsite certChains.

Definition at line 38 of file https.py.

6.11.3 Variable Documentation

6.11.3.1 rpki::https.debug_tls_certs = False

Definition at line 34 of file https.py.

6.11.3.2 rpki::https.disable_tls_certificate_validation_exceptions = False

Definition at line 31 of file https.py.

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

Definition at line 36 of file https.py.

6.12 Package rpki.ipaddr

Classes

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

6.12.1 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: ipaddr.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 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

6.13.1 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.

6.13.2 Variable Documentation

6.13.2.1 `rpki::left_right.enforce_strict_up_down_xml_sender = False`

Definition at line 26 of file `left_right.py`.

6.14 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)`

6.14.1 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.

6.14.2 Function Documentation

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

Initialize logging system.

Definition at line 27 of file log.py.

6.14.2.2 `def rpki.log.set_trace (trace)`

Enable or disable call tracing.

Definition at line 32 of file log.py.

6.14.2.3 `def rpki.log.trace ()`

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

Definition at line 53 of file log.py.

6.14.3 Variable Documentation

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

Definition at line 51 of file log.py.

6.14.3.2 `rpki::log::enable_trace = False`

Whether call tracing is enabled.

Definition at line 25 of file log.py.

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

Definition at line 47 of file log.py.

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

Definition at line 50 of file log.py.

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

Definition at line 49 of file log.py.

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

Definition at line 48 of file log.py.

6.15 Package rpki.manifest

Classes

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

6.15.1 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.

6.16 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.

6.16.1 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.

6.16.2 Variable Documentation

6.16.2.1 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.

6.16.2.2 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.

6.17 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.

6.17.1 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.

6.17.2 Variable Documentation

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

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

Definition at line 232 of file publication.py.

6.18 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.

6.18.1 Variable Documentation

6.18.1.1 `rpki::relaxng::left_right`

Parsed RelaxNG [left_right](#) schema.

Definition at line 7 of file relaxng.py.

6.18.1.2 `rpki::relaxng::publication`

Parsed RelaxNG [publication](#) schema.

Definition at line 1214 of file relaxng.py.

6.18.1.3 rpki::relaxng::up_down

Parsed RelaxNG [up_down](#) schema.

Definition at line 960 of file relaxng.py.

6.19 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.

6.19.1 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.

6.19.2 Function Documentation

6.19.2.1 `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`.

6.19.2.2 `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`.

6.19.2.3 `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`.

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

Definition at line 731 of file resource_set.py.

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

Definition at line 764 of file resource_set.py.

6.19.3 Variable Documentation**6.19.3.1 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.

6.20 Package rpki.roa**Classes**

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

6.20.1 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
```

6.21 Package rpki.rpki_engine

Classes

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

6.21.1 Detailed Description

Global context for rpkiid.

\$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.

6.22 Package rpki.sql

Classes

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

6.22.1 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.

6.23 Package rpki.sundial

Classes

- class `datetime`
- class `timedelta`

Functions

- def `now`
- def `test`

6.23.1 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.

6.23.2 Function Documentation

6.23.2.1 def rpki.sundial.now ()

Get current timestamp.

Definition at line 26 of file sundial.py.

6.23.2.2 def rpki.sundial.test (t)

Definition at line 174 of file sundial.py.

6.24 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/"

6.24.1 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.

6.24.2 Variable Documentation

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

Definition at line 26 of file `up_down.py`.

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

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

6.25 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](#)

6.25.1 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.

6.25.2 Function Documentation

6.25.2.1 `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.

6.25.2.2 `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.

6.26 Package rpki.xml_utils

Classes

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

6.26.1 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.
```

6.27 Package rpkiid

Functions

- def `main`

Variables

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

6.27.1 Detailed Description

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

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

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

```
$Id: rpkiid.py 1880 2008-06-12 21:54:53Z 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.

6.27.2 Function Documentation

6.27.2.1 `def rpkid.main ()`

Definition at line 52 of file rpkid.py.

6.27.3 Variable Documentation

6.27.3.1 `rpkid.cfg_file = "rpkid.conf"`

Definition at line 37 of file rpkid.py.

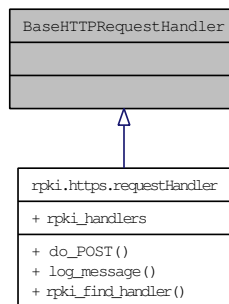
6.27.3.2 `rpkid.profile = None`

Definition at line 38 of file rpkid.py.

7 Class Documentation

7.1 BaseHTTPRequestHandler Class Reference

Inheritance diagram for BaseHTTPRequestHandler:

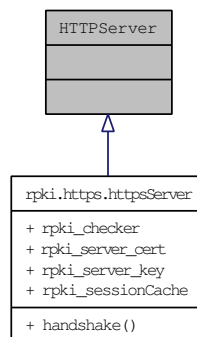


The documentation for this class was generated from the following file:

- [https.py \(1873\)](#)

7.2 HTTPServer Class Reference

Inheritance diagram for HTTPServer:

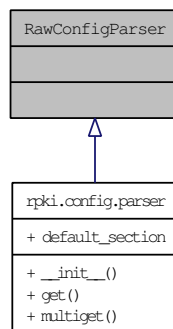


The documentation for this class was generated from the following file:

- [https.py \(1873\)](#)

7.3 RawConfigParser Class Reference

Inheritance diagram for RawConfigParser:

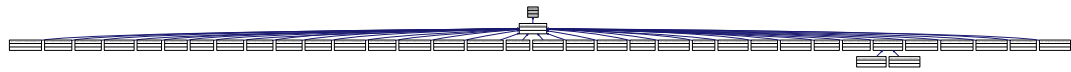


The documentation for this class was generated from the following file:

- [config.py \(1873\)](#)

7.4 Exception Class Reference

Inheritance diagram for Exception:

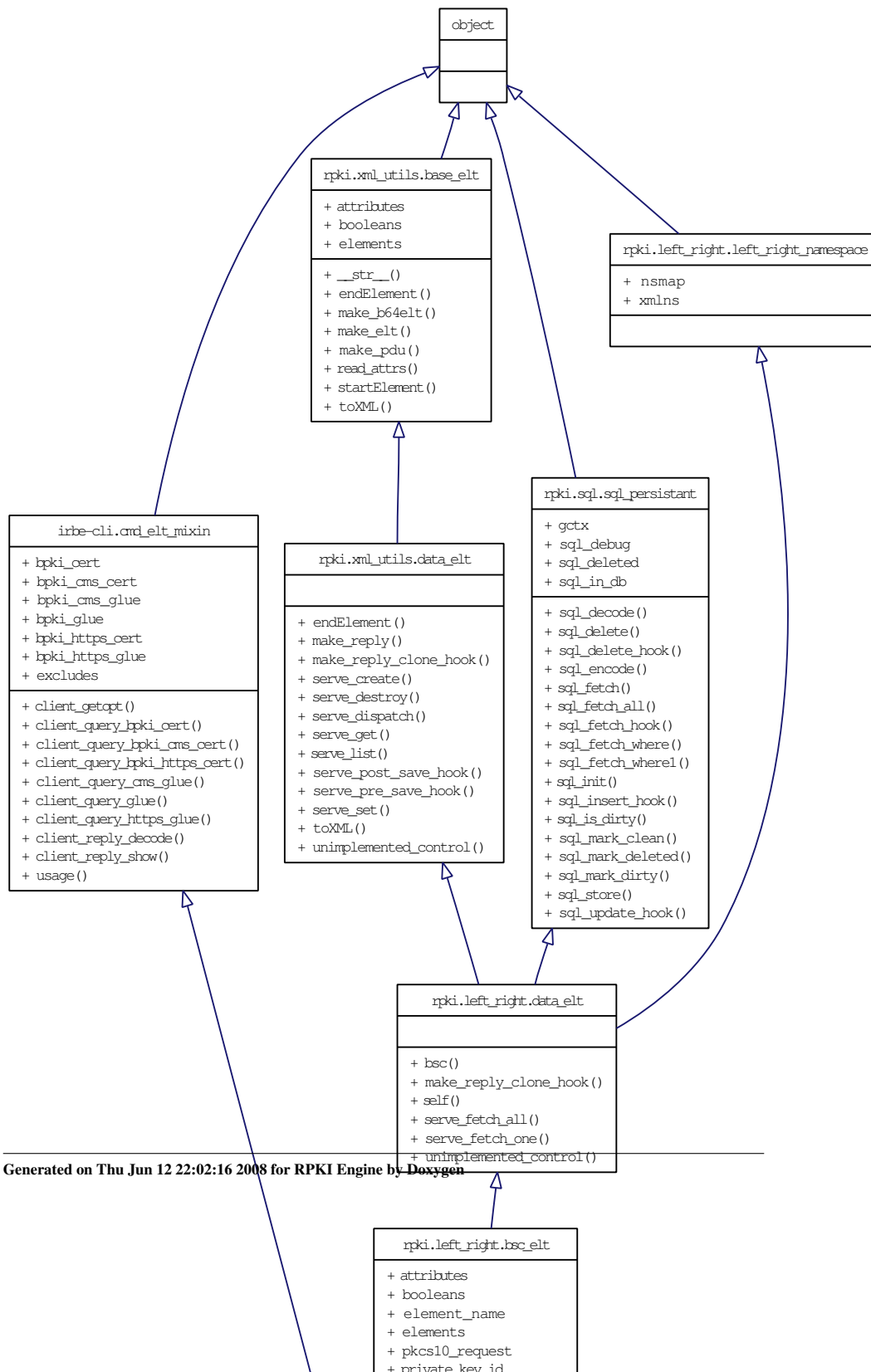


The documentation for this class was generated from the following file:

- [exceptions.py \(1873\)](#)

7.5 irbe-cli.bsc_elt Class Reference

Inheritance diagram for irbe-cli.bsc_elt:



Public Member Functions

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

Public Attributes

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

Static Public Attributes

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

7.5.1 Detailed Description

Definition at line 117 of file irbe-cli.py.

7.5.2 Member Function Documentation

7.5.2.1 def irbe-cli.bsc_elt.client_query_signing_cert (self, arg)

--signing_cert option.

Definition at line 121 of file irbe-cli.py.

7.5.2.2 def irbe-cli.bsc_elt.client_query_signing_cert_crl (self, arg)

--signing_cert_crl option.

Definition at line 125 of file irbe-cli.py.

7.5.2.3 def irbe-cli.bsc_elt.client_reply_decode (self)

Reimplemented from [irbe-cli.cmd_elt_mixin](#).

Definition at line 129 of file irbe-cli.py.

7.5.3 Member Data Documentation

7.5.3.1 tuple irbe-cli.bsc_elt.excludes = ("pkcs10_request",) [static]

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

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

Reimplemented from [irbe-cli.cmd_elt_mixin](#).

Definition at line 119 of file irbe-cli.py.

7.5.3.2 irbe-cli.bsc_elt.signing_cert

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

Definition at line 123 of file irbe-cli.py.

7.5.3.3 irbe-cli.bsc_elt.signing_cert_crl

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

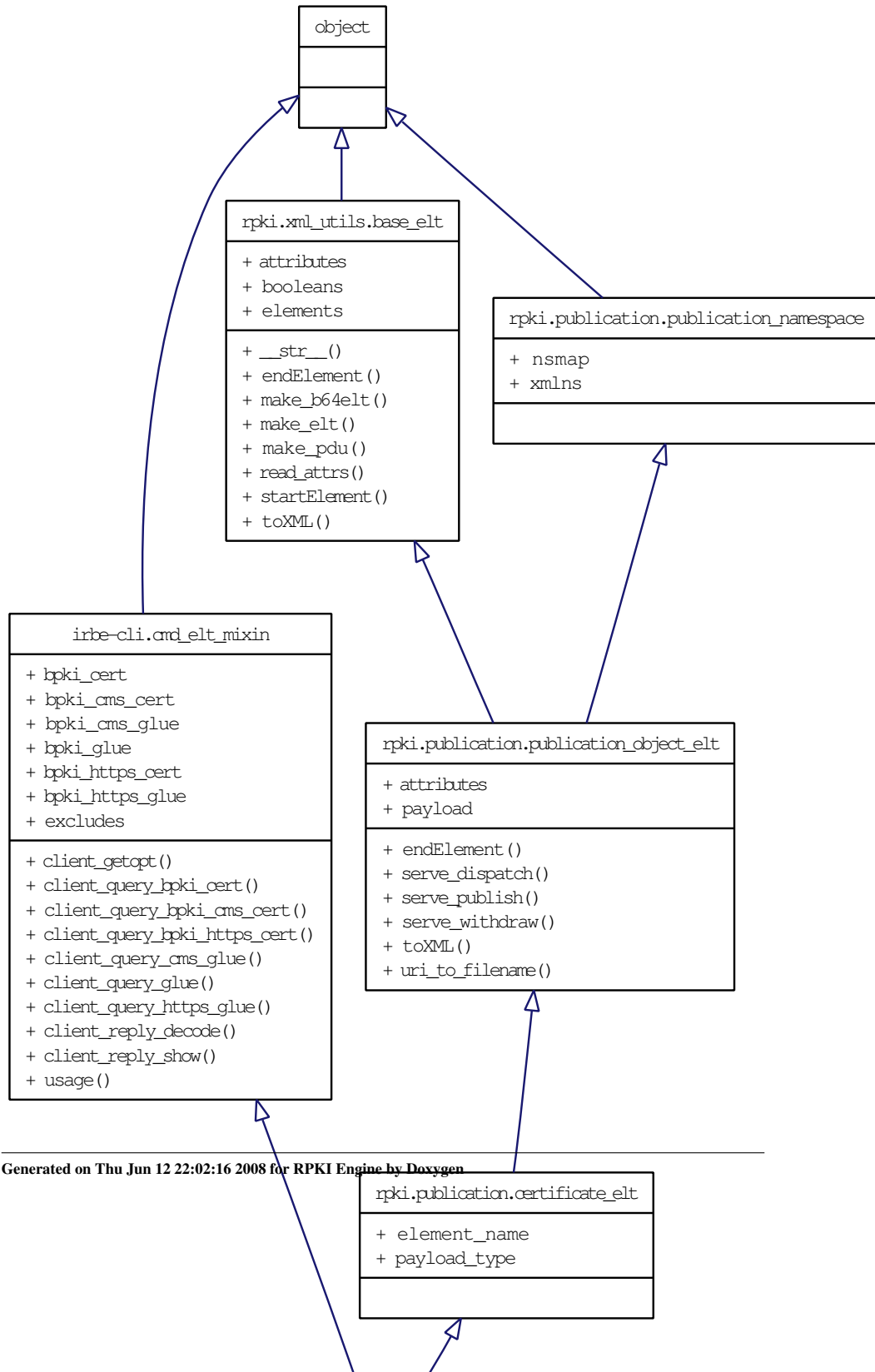
Definition at line 127 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.6 irbe-cli.certificate_elt Class Reference

Inheritance diagram for irbe-cli.certificate_elt:



7.6.1 Detailed Description

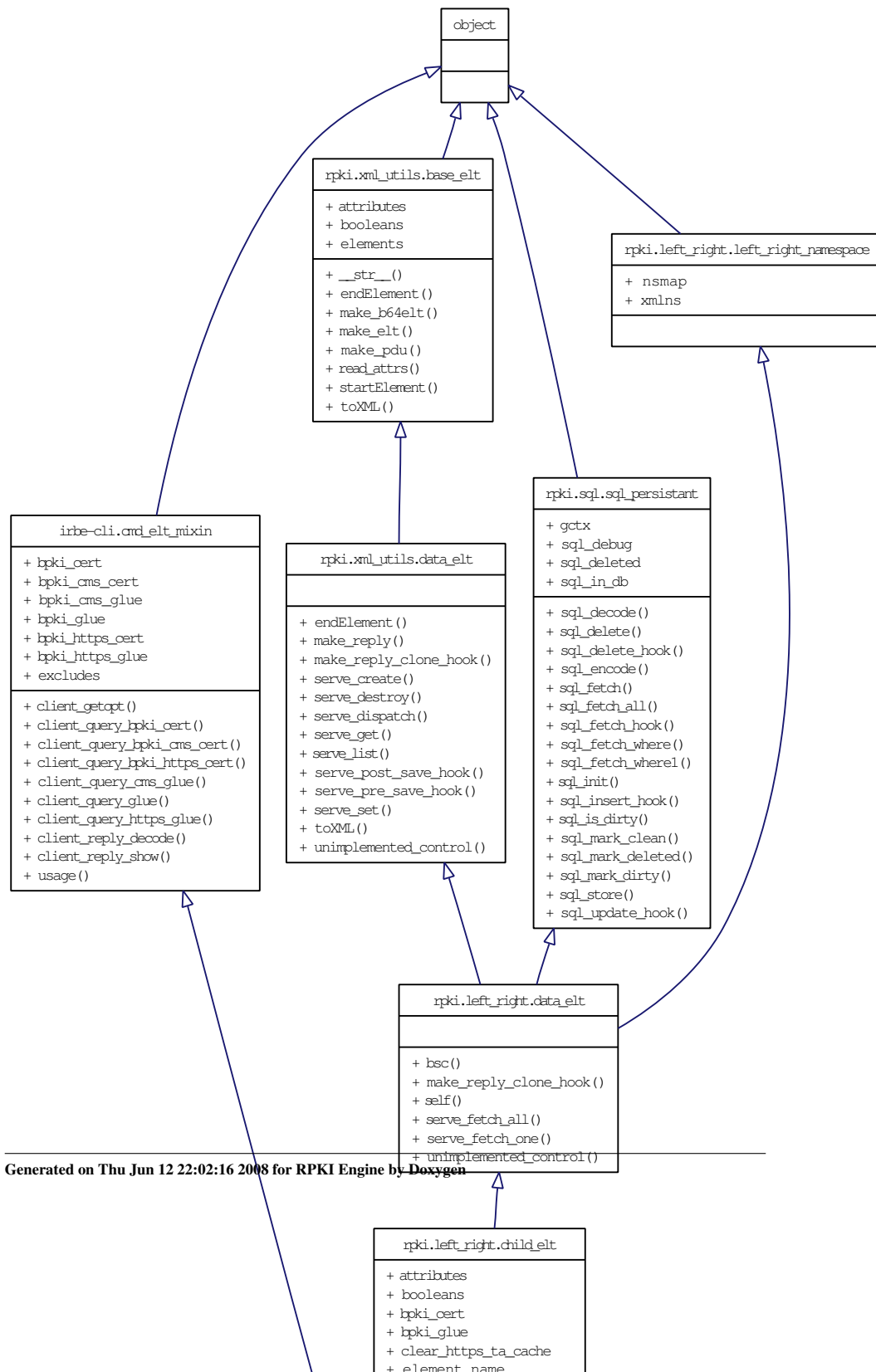
Definition at line 180 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.7 irbe-cli.child_elt Class Reference

Inheritance diagram for irbe-cli.child_elt:



7.7.1 Detailed Description

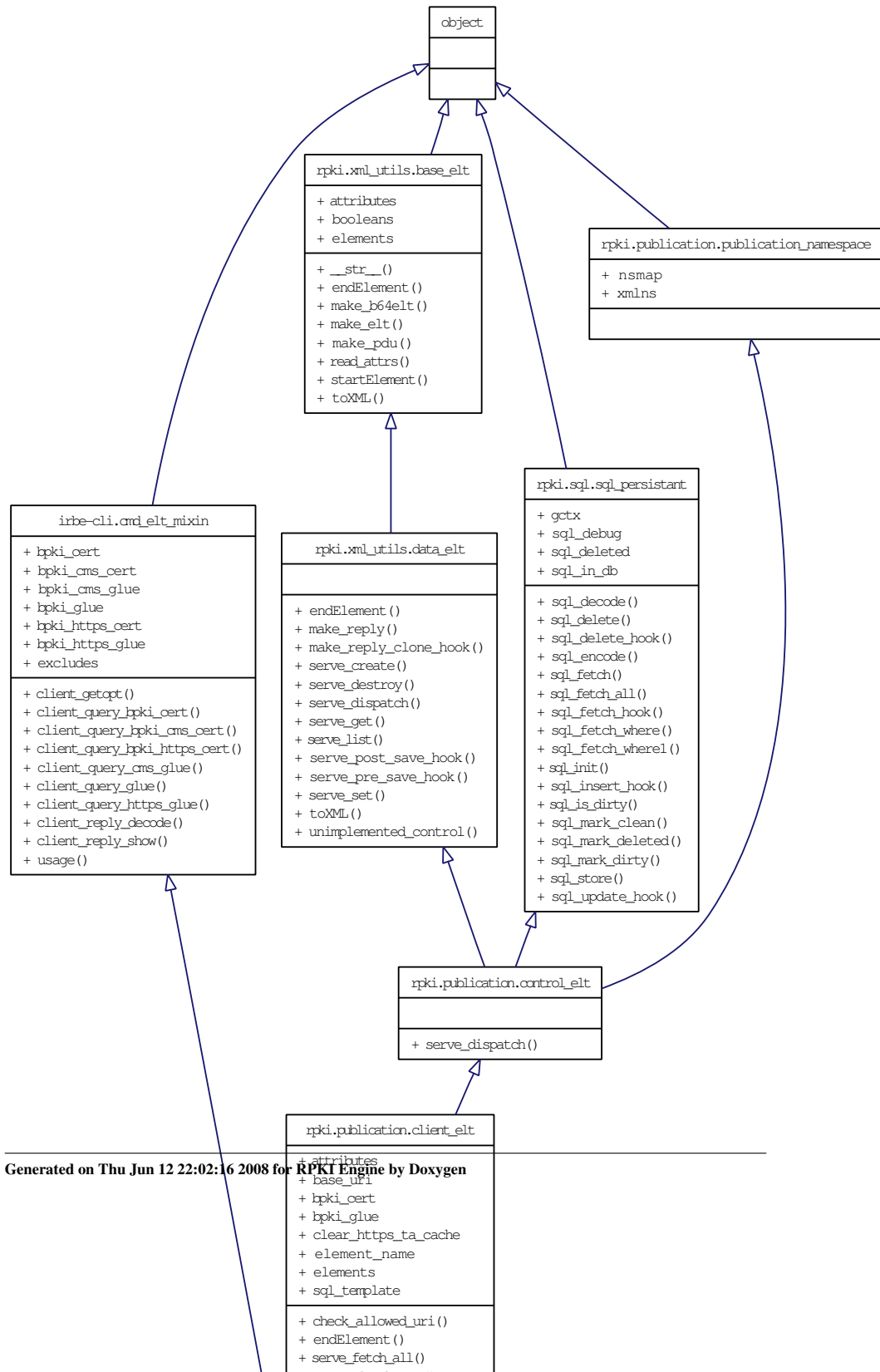
Definition at line 139 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.8 irbe-cli.client_elt Class Reference

Inheritance diagram for irbe-cli.client_elt:



- [bpki_glue](#)
- [bpki_https_cert](#)
- [bpki_https_glue](#)

Static Public Attributes

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

7.9.1 Detailed Description

Protocol mix-in for command line client element PDUs.

Definition at line 35 of file `irbe-cli.py`.

7.9.2 Member Function Documentation

7.9.2.1 `def irbe-cli.cmd_elt_mixin.client_getopt (self, argv)`

Parse options for this class.

Definition at line 55 of file `irbe-cli.py`.

7.9.2.2 `def irbe-cli.cmd_elt_mixin.client_query_bpki_cert (self, arg)`

Special handler for `--bpki_cert` option.

Definition at line 70 of file `irbe-cli.py`.

7.9.2.3 `def irbe-cli.cmd_elt_mixin.client_query_bpki_cms_cert (self, arg)`

Special handler for `--bpki_cms_cert` option.

Definition at line 78 of file `irbe-cli.py`.

7.9.2.4 `def irbe-cli.cmd_elt_mixin.client_query_bpki_https_cert (self, arg)`

Special handler for `--bpki_https_cert` option.

Definition at line 86 of file `irbe-cli.py`.

7.9.2.5 def irbe-cli.cmd_elt_mixin.client_query_cms_glue (self, arg)

Special handler for --bpki_cms_glue option.

Definition at line 82 of file irbe-cli.py.

7.9.2.6 def irbe-cli.cmd_elt_mixin.client_query_glue (self, arg)

Special handler for --bpki_glue option.

Definition at line 74 of file irbe-cli.py.

7.9.2.7 def irbe-cli.cmd_elt_mixin.client_query_https_glue (self, arg)

Special handler for --bpki_https_glue option.

Definition at line 90 of file irbe-cli.py.

7.9.2.8 def irbe-cli.cmd_elt_mixin.client_reply_decode (self)

Reimplemented in [irbe-cli.bsc_elt](#).

Definition at line 94 of file irbe-cli.py.

7.9.2.9 def irbe-cli.cmd_elt_mixin.client_reply_show (self)

Definition at line 97 of file irbe-cli.py.

7.9.2.10 def irbe-cli.cmd_elt_mixin.usage (cls)

Generate usage message for this PDU.

Definition at line 46 of file irbe-cli.py.

7.9.3 Member Data Documentation**7.9.3.1 irbe-cli.cmd_elt_mixin.bpki_cert**

Definition at line 72 of file irbe-cli.py.

7.9.3.2 irbe-cli.cmd_elt_mixin.bpki_cms_cert

Definition at line 80 of file irbe-cli.py.

7.9.3.3 irbe-cli.cmd_elt_mixin.bpki_cms_glue

Definition at line 84 of file irbe-cli.py.

7.9.3.4 irbe-cli.cmd_elt_mixin.bpki_glue

Definition at line 76 of file irbe-cli.py.

7.9.3.5 irbe-cli.cmd_elt_mixin.bpki_https_cert

Definition at line 88 of file irbe-cli.py.

7.9.3.6 irbe-cli.cmd_elt_mixin.bpki_https_glue

Definition at line 92 of file irbe-cli.py.

7.9.3.7 irbe-cli.cmd_elt_mixin::excludes = () [static]

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

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

Reimplemented in [irbe-cli.bsc_elt](#).

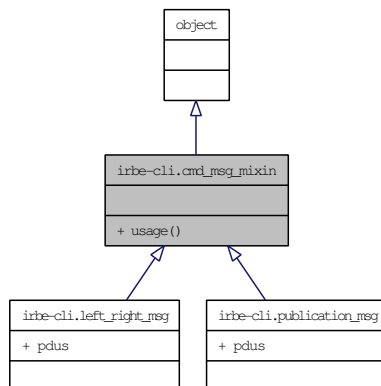
Definition at line 43 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.10 irbe-cli.cmd_msg_mixin Class Reference

Inheritance diagram for irbe-cli.cmd_msg_mixin:



Public Member Functions

- def [usage](#)

7.10.1 Detailed Description

Protocol mix-in for command line client message PDUs.

Definition at line 103 of file irbe-cli.py.

7.10.2 Member Function Documentation

7.10.2.1 def irbe-cli.cmd_msg_mixin.usage (cls)

Generate usage message for this PDU.

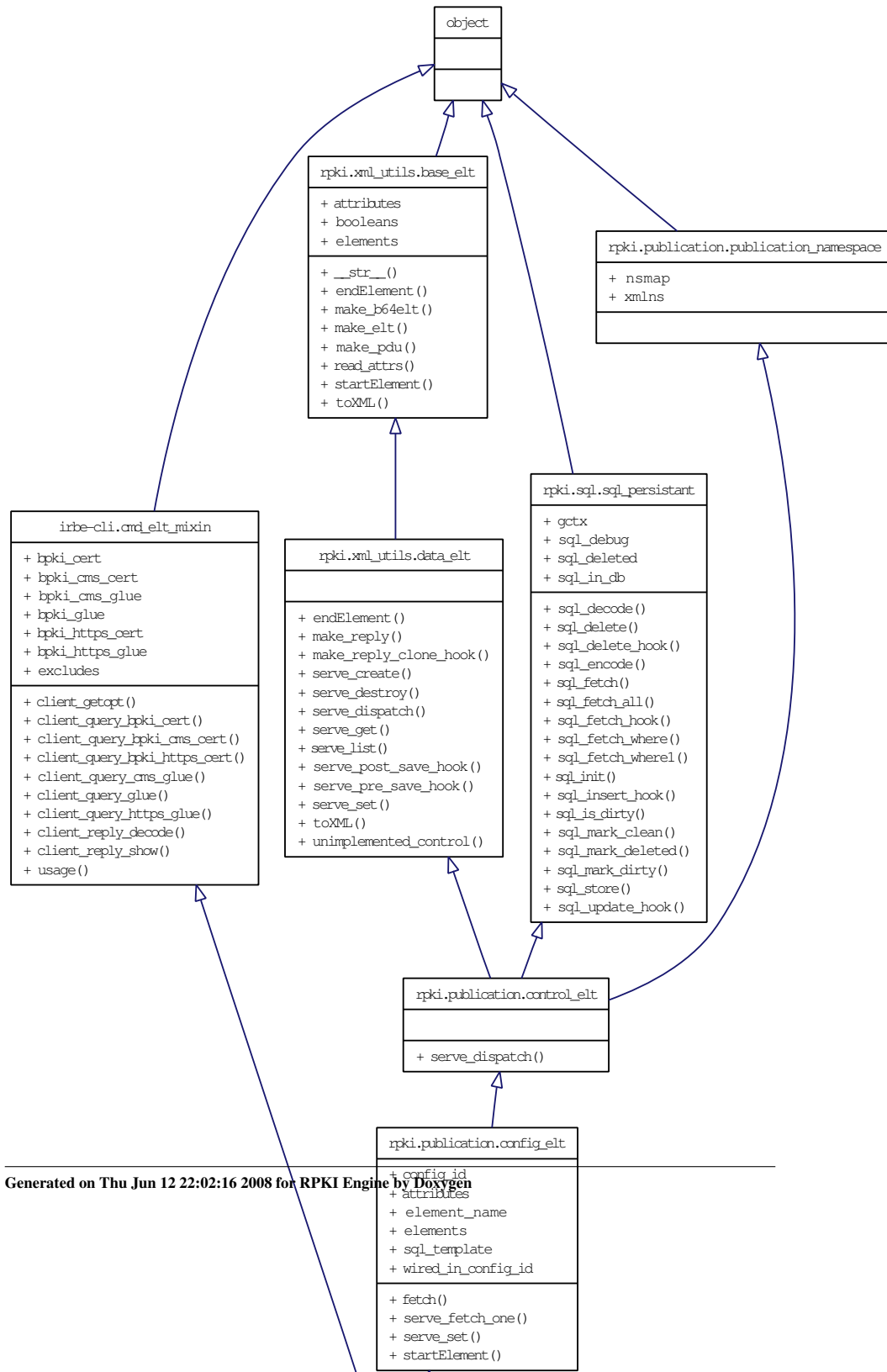
Definition at line 107 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.11 irbe-cli.config_elt Class Reference

Inheritance diagram for irbe-cli.config_elt:



Public Member Functions

- def [client_query_bpki_crl](#)

Public Attributes

- [bpki_crl](#)

7.11.1 Detailed Description

Definition at line 171 of file irbe-cli.py.

7.11.2 Member Function Documentation

7.11.2.1 def irbe-cli.config_elt.client_query_bpki_crl (*self*, *arg*)

Special handler for --bpki_crl option.

Definition at line 173 of file irbe-cli.py.

7.11.3 Member Data Documentation

7.11.3.1 irbe-cli.config_elt.bpki_crl

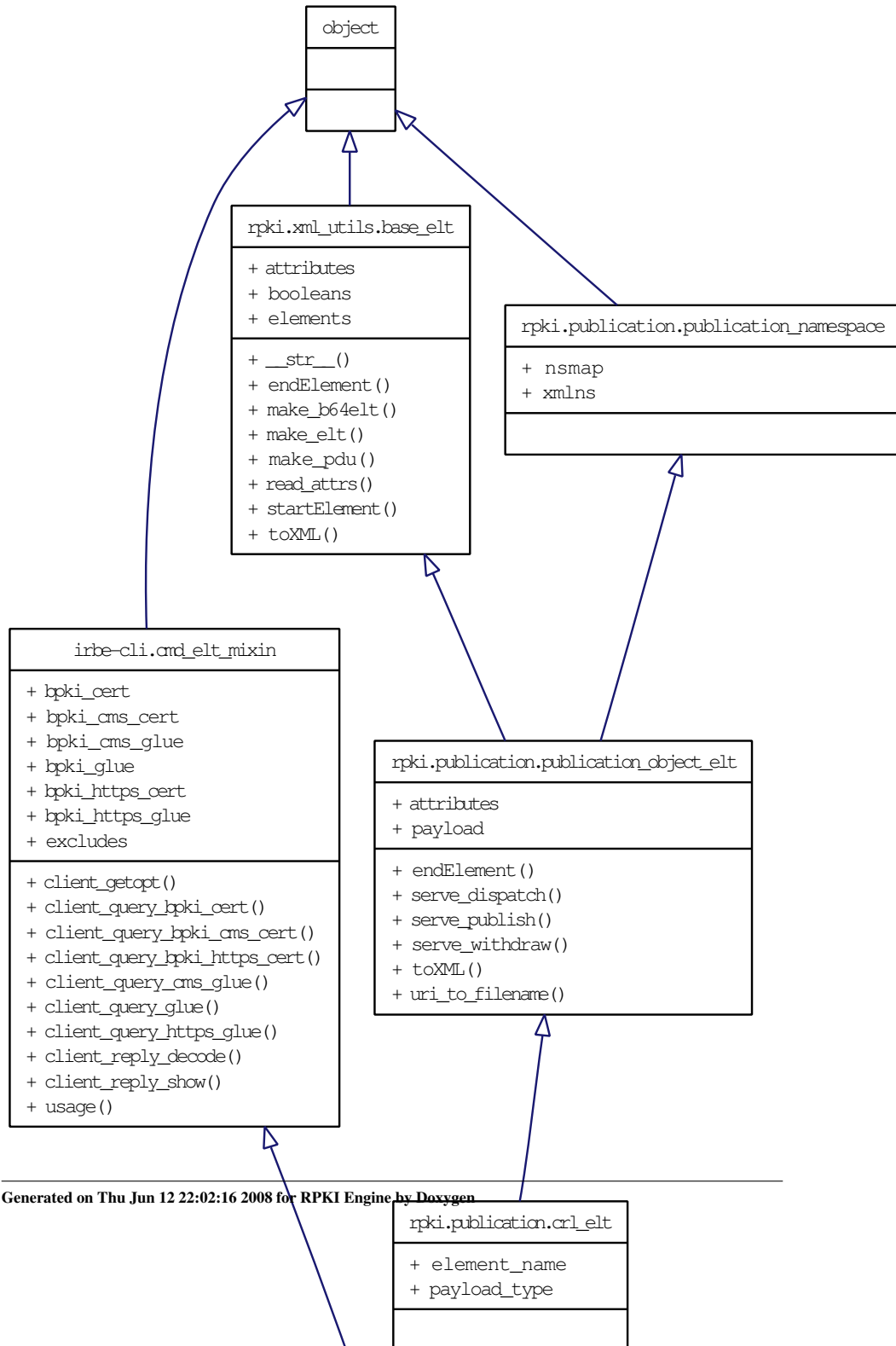
Definition at line 175 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.12 irbe-cli.crl_elt Class Reference

Inheritance diagram for irbe-cli.crl_elt:



7.12.1 Detailed Description

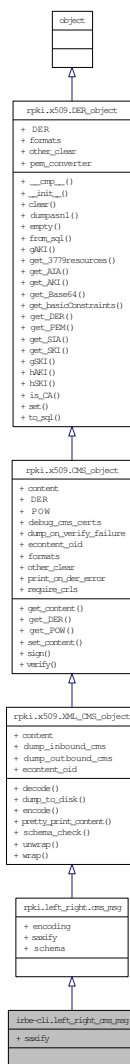
Definition at line 183 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.13 irbe-cli.left_right_cms_msg Class Reference

Inheritance diagram for irbe-cli.left_right_cms_msg:



Static Public Attributes

- [saxify](#) = left_right_sax_handler.saxify

7.13.1 Detailed Description

Definition at line 166 of file irbe-cli.py.

7.13.2 Member Data Documentation

7.13.2.1 irbe-cli.left_right_cms_msg.saxify = **left_right_sax_handler.saxify**
[static]

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

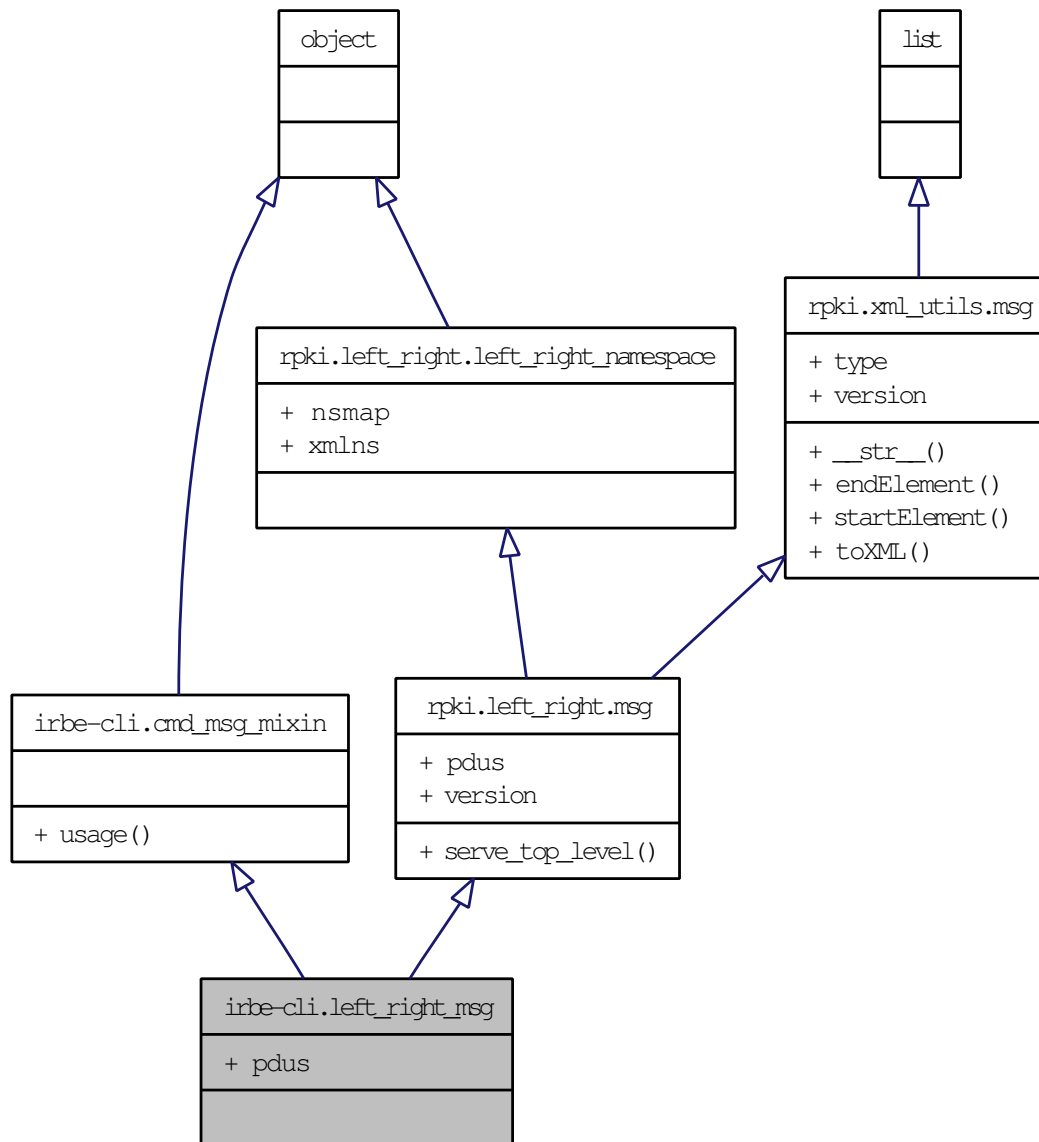
Definition at line 167 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.14 irbe-cli.left_right_msg Class Reference

Inheritance diagram for irbe-cli.left_right_msg:



Static Public Attributes

- tuple `pdus`

Dispatch table of PDUs for this protocol.

7.14.1 Detailed Description

Definition at line 159 of file irbe-cli.py.

7.14.2 Member Data Documentation

7.14.2.1 tuple irbe-cli.left_right_msg.pdus [static]

Initial value:

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

Dispatch table of PDUs for this protocol.

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

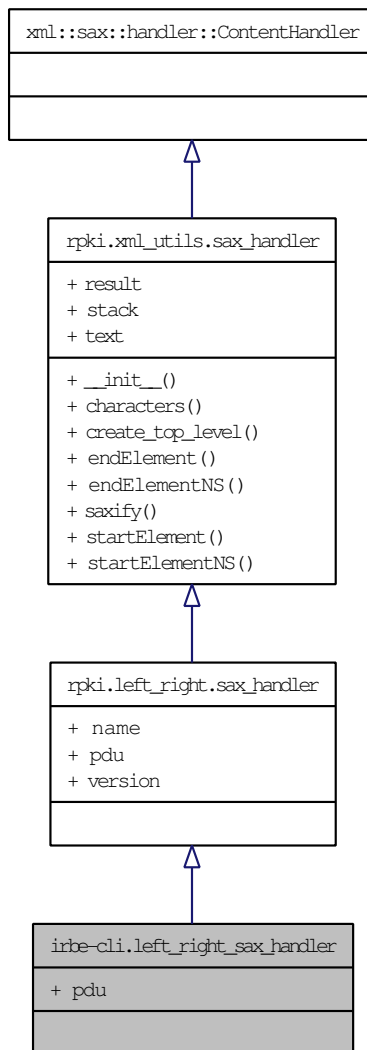
Definition at line 160 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.15 irbe-cli.left_right_sax_handler Class Reference

Inheritance diagram for irbe-cli.left_right_sax_handler:



Static Public Attributes

- `pdu = left_right_msg`

7.15.1 Detailed Description

Definition at line 163 of file irbe-cli.py.

7.15.2 Member Data Documentation

7.15.2.1 irbe-cli.left_right_sax_handler.pdu = left_right_msg [static]

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

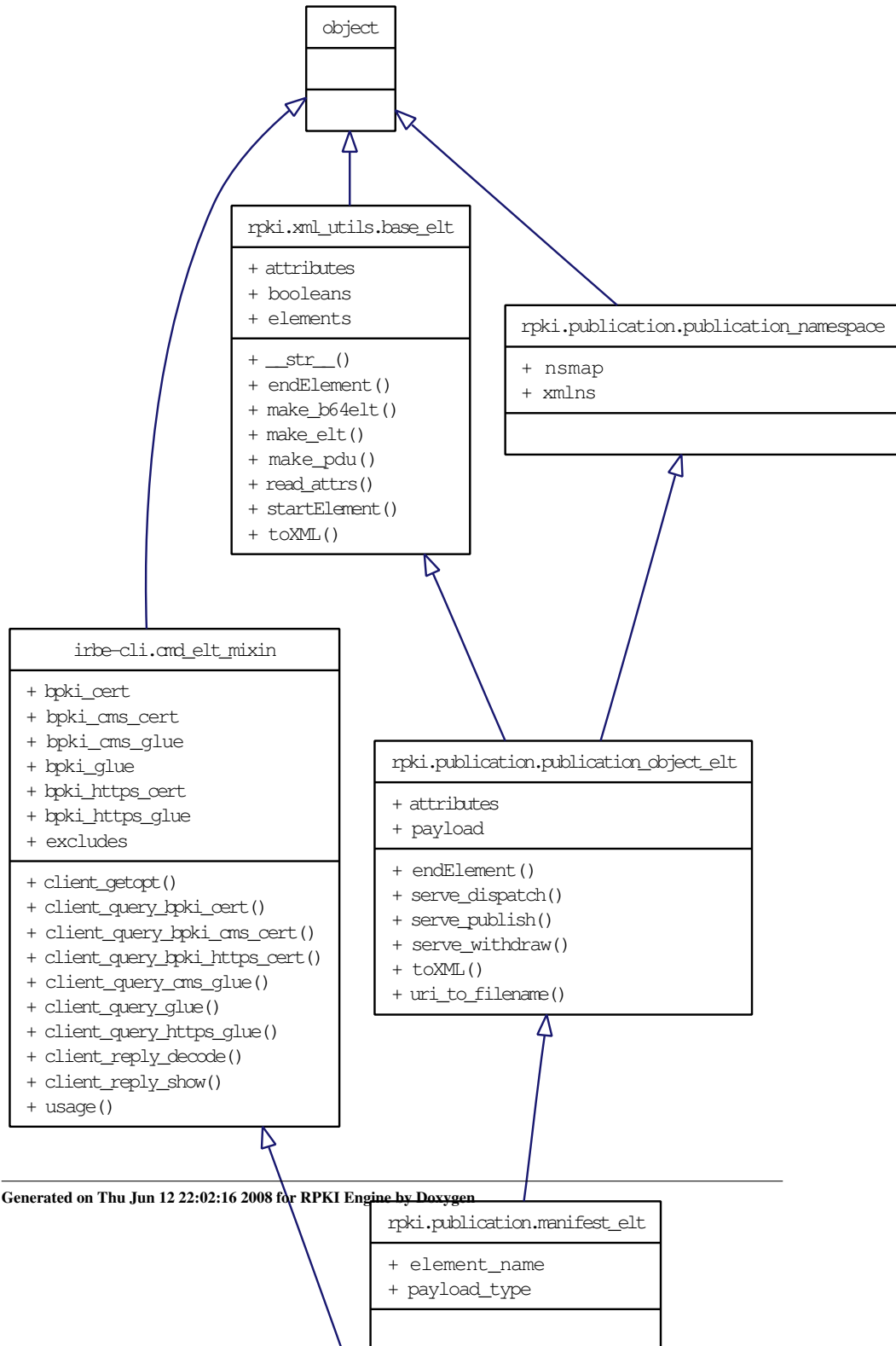
Definition at line 164 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.16 irbe-cli.manifest_elt Class Reference

Inheritance diagram for irbe-cli.manifest_elt:



7.16.1 Detailed Description

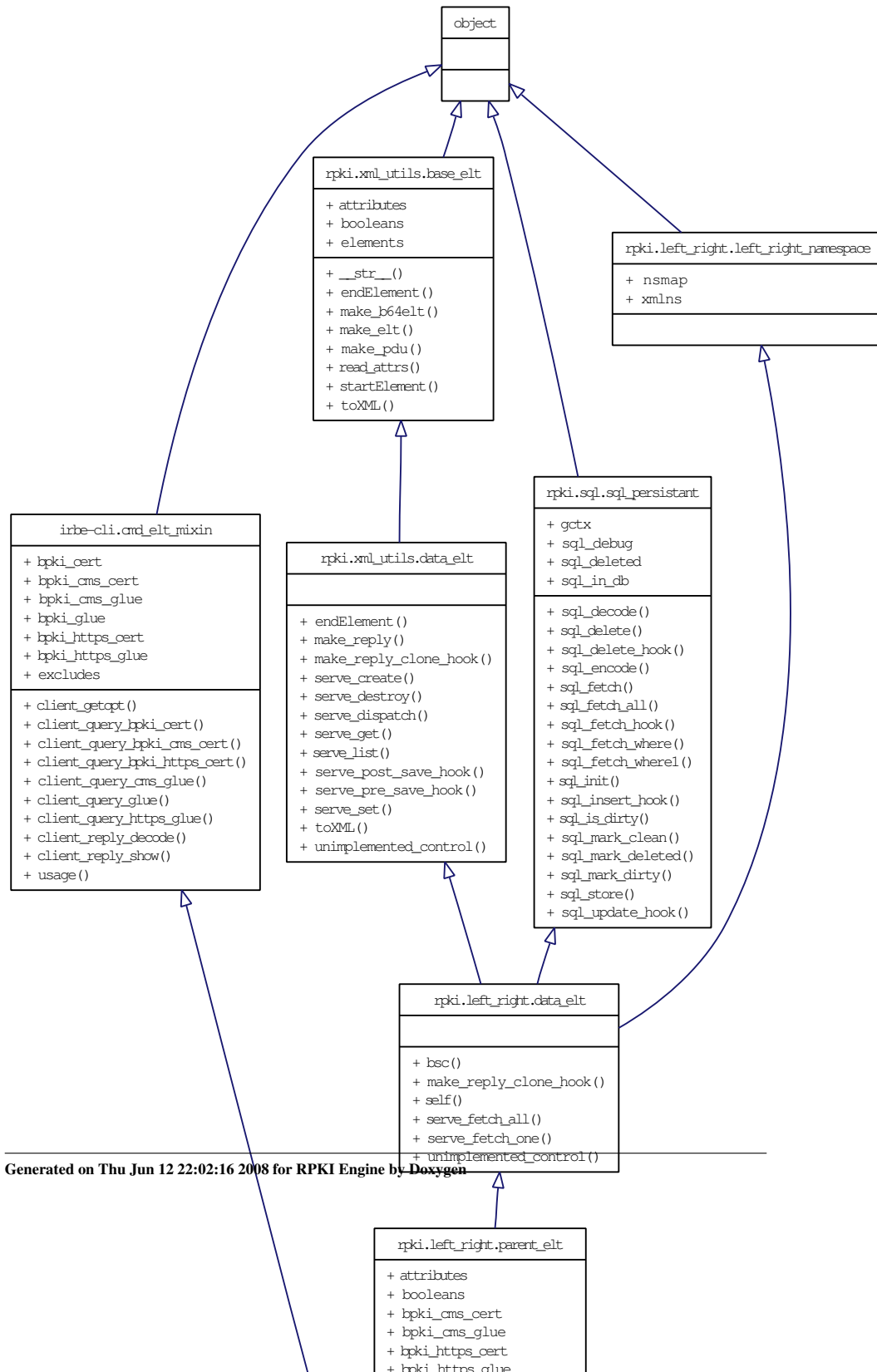
Definition at line 186 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.17 irbe-cli.parent_elt Class Reference

Inheritance diagram for irbe-cli.parent_elt:



7.17.1 Detailed Description

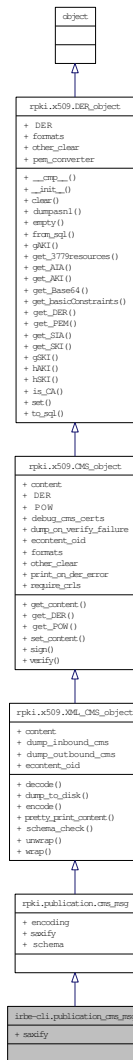
Definition at line 136 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.18 irbe-cli.publication_cms_msg Class Reference

Inheritance diagram for irbe-cli.publication_cms_msg:



Static Public Attributes

- `saxify` = `publication_sax_handler.saxify`

7.18.1 Detailed Description

Definition at line 199 of file `irbe-cli.py`.

7.18.2 Member Data Documentation

7.18.2.1 `irbe-cli.publication_cms_msg.saxify = publication_sax_handler.saxify` [static]

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

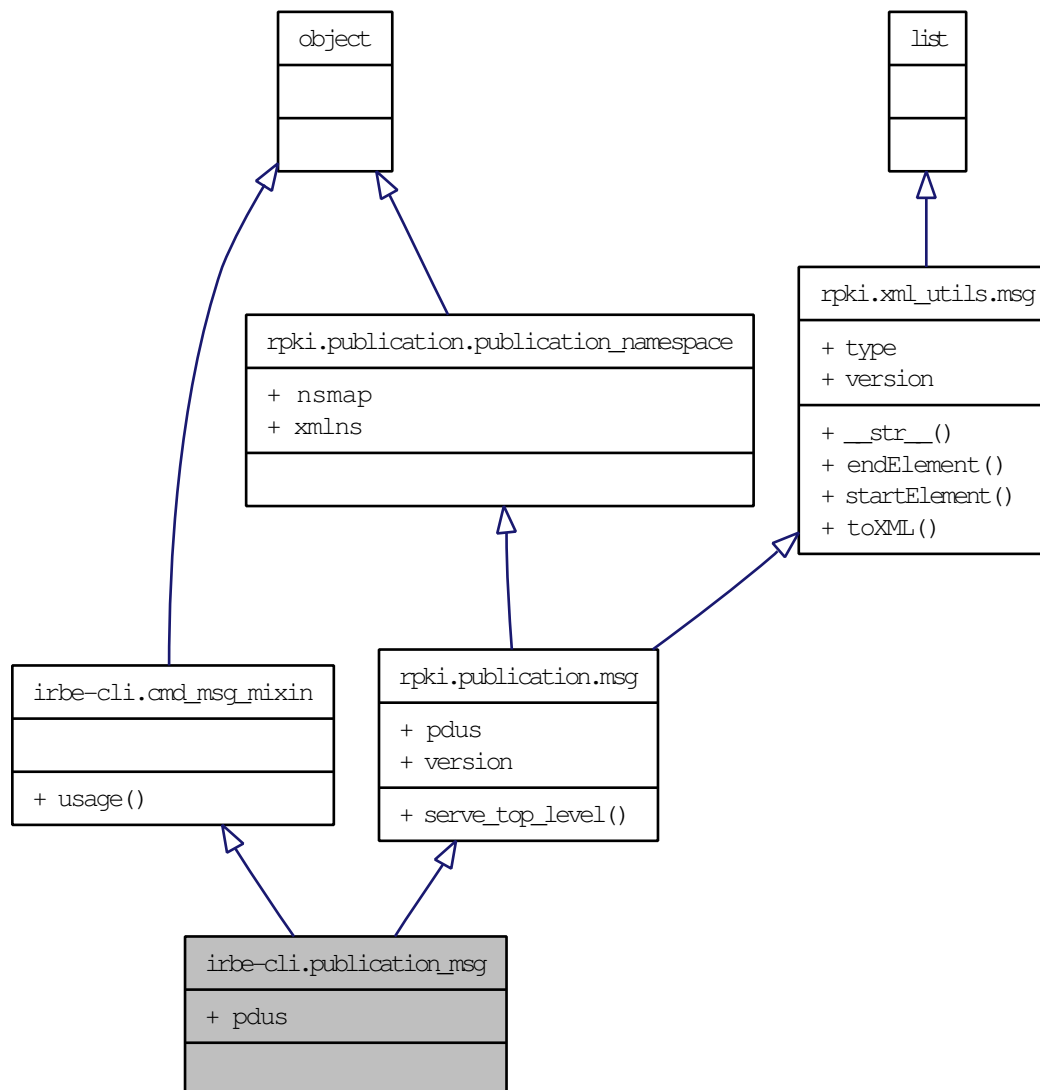
Definition at line 200 of file `irbe-cli.py`.

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

- [irbe-cli.py \(1880\)](#)

7.19 irbe-cli.publication_msg Class Reference

Inheritance diagram for irbe-cli.publication_msg:



Static Public Attributes

- tuple `pdus`

Dispatch table of PDUs for this protocol.

7.19.1 Detailed Description

Definition at line 192 of file irbe-cli.py.

7.19.2 Member Data Documentation

7.19.2.1 tuple irbe-cli.publication_msg.pdus [static]

Initial value:

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

Dispatch table of PDUs for this protocol.

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

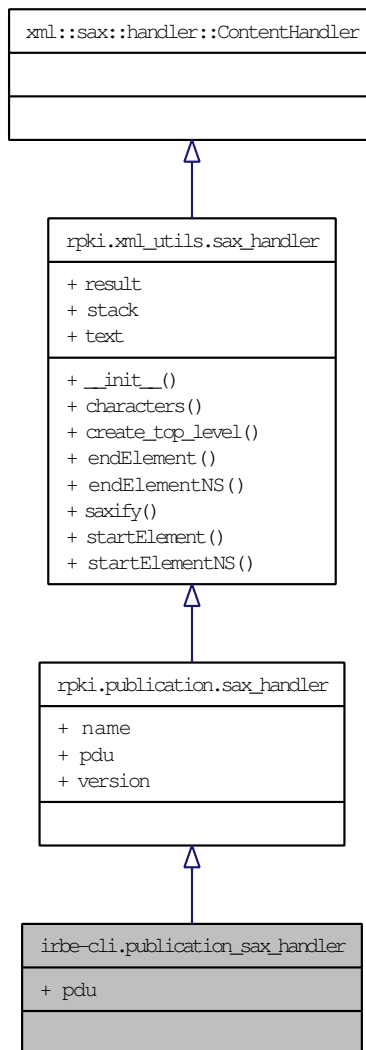
Definition at line 193 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.20 irbe-cli.publication_sax_handler Class Reference

Inheritance diagram for irbe-cli.publication_sax_handler:



Static Public Attributes

- `pdu = publication_msg`

7.20.1 Detailed Description

Definition at line 196 of file `irbe-cli.py`.

7.20.2 Member Data Documentation

7.20.2.1 `irbe-cli.publication_sax_handler.pdu = publication_msg` [static]

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

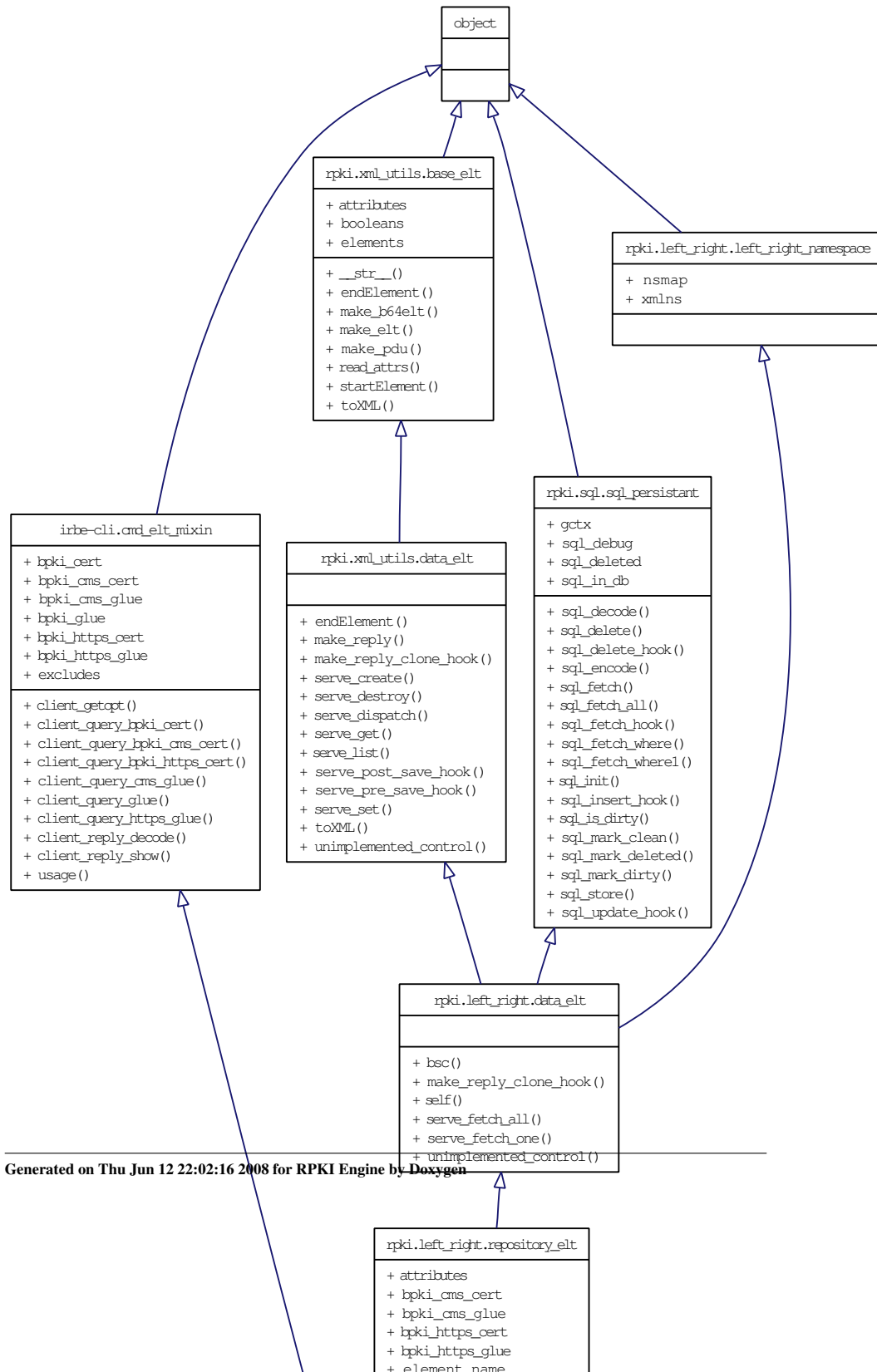
Definition at line 197 of file `irbe-cli.py`.

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

- [irbe-cli.py \(1880\)](#)

7.21 irbe-cli.repository_elt Class Reference

Inheritance diagram for irbe-cli.repository_elt:



7.21.1 Detailed Description

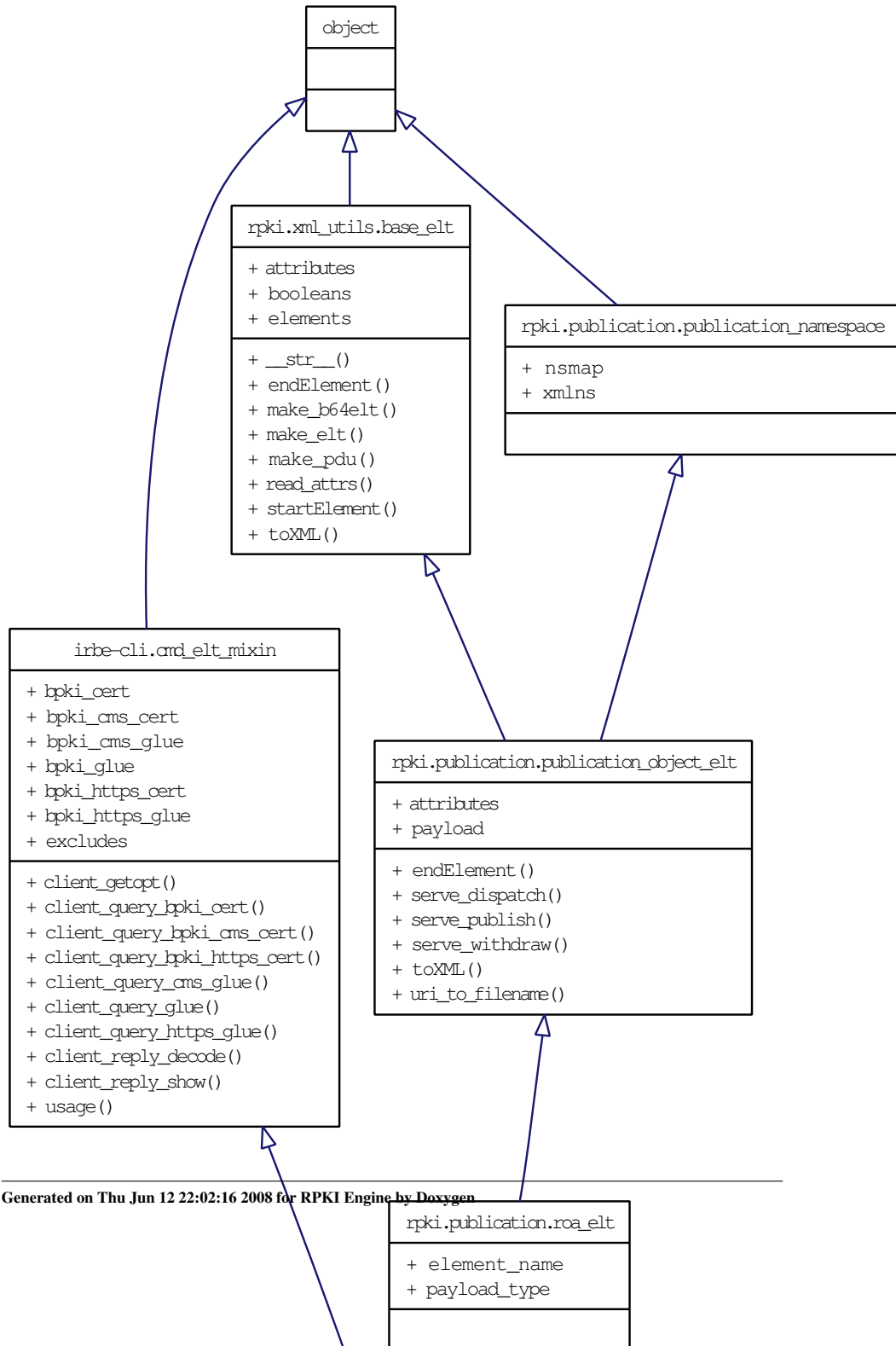
Definition at line 142 of file `irbe-cli.py`.

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

- [irbe-cli.py \(1880\)](#)

7.22 irbe-cli.roa_elt Class Reference

Inheritance diagram for irbe-cli.roa_elt:



7.22.1 Detailed Description

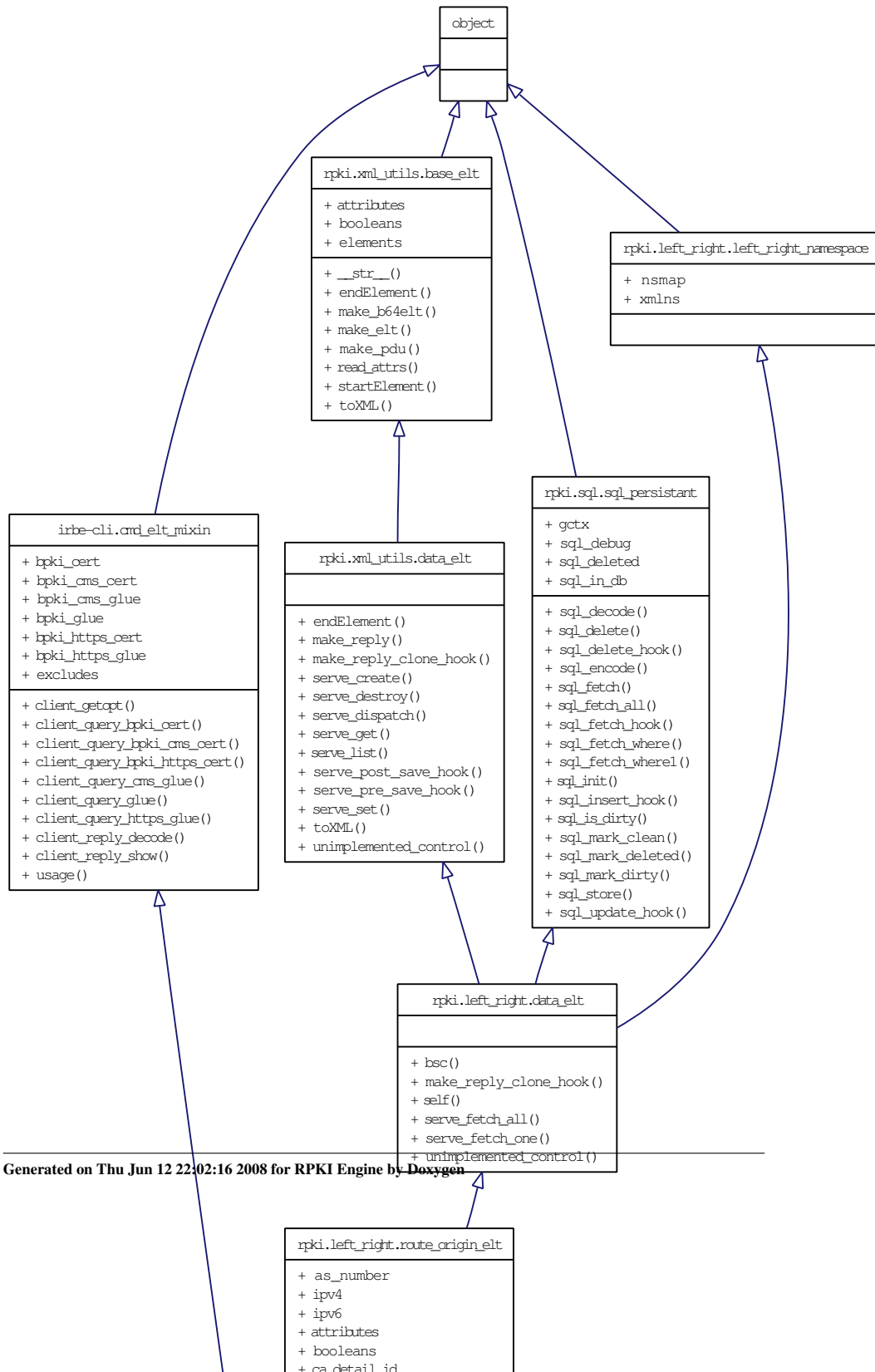
Definition at line 189 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.23 irbe-cli.route_origin_elt Class Reference

Inheritance diagram for irbe-cli.route_origin_elt:



Public Member Functions

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

Public Attributes

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

7.23.1 Detailed Description

Definition at line 145 of file irbe-cli.py.

7.23.2 Member Function Documentation

7.23.2.1 def irbe-cli.route_origin_elt.client_query_as_number (self, arg)

Handle autonomous sequence numbers.

Definition at line 147 of file irbe-cli.py.

7.23.2.2 def irbe-cli.route_origin_elt.client_query_ipv4 (self, arg)

Handle IPv4 addresses.

Definition at line 151 of file irbe-cli.py.

7.23.2.3 def irbe-cli.route_origin_elt.client_query_ipv6 (self, arg)

Handle IPv6 addresses.

Definition at line 155 of file irbe-cli.py.

7.23.3 Member Data Documentation

7.23.3.1 irbe-cli.route_origin_elt.as_number

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

Definition at line 149 of file irbe-cli.py.

7.23.3.2 `irbe-cli.route_origin_elt.ipv4`

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

Definition at line 153 of file `irbe-cli.py`.

7.23.3.3 `irbe-cli.route_origin_elt.ipv6`

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

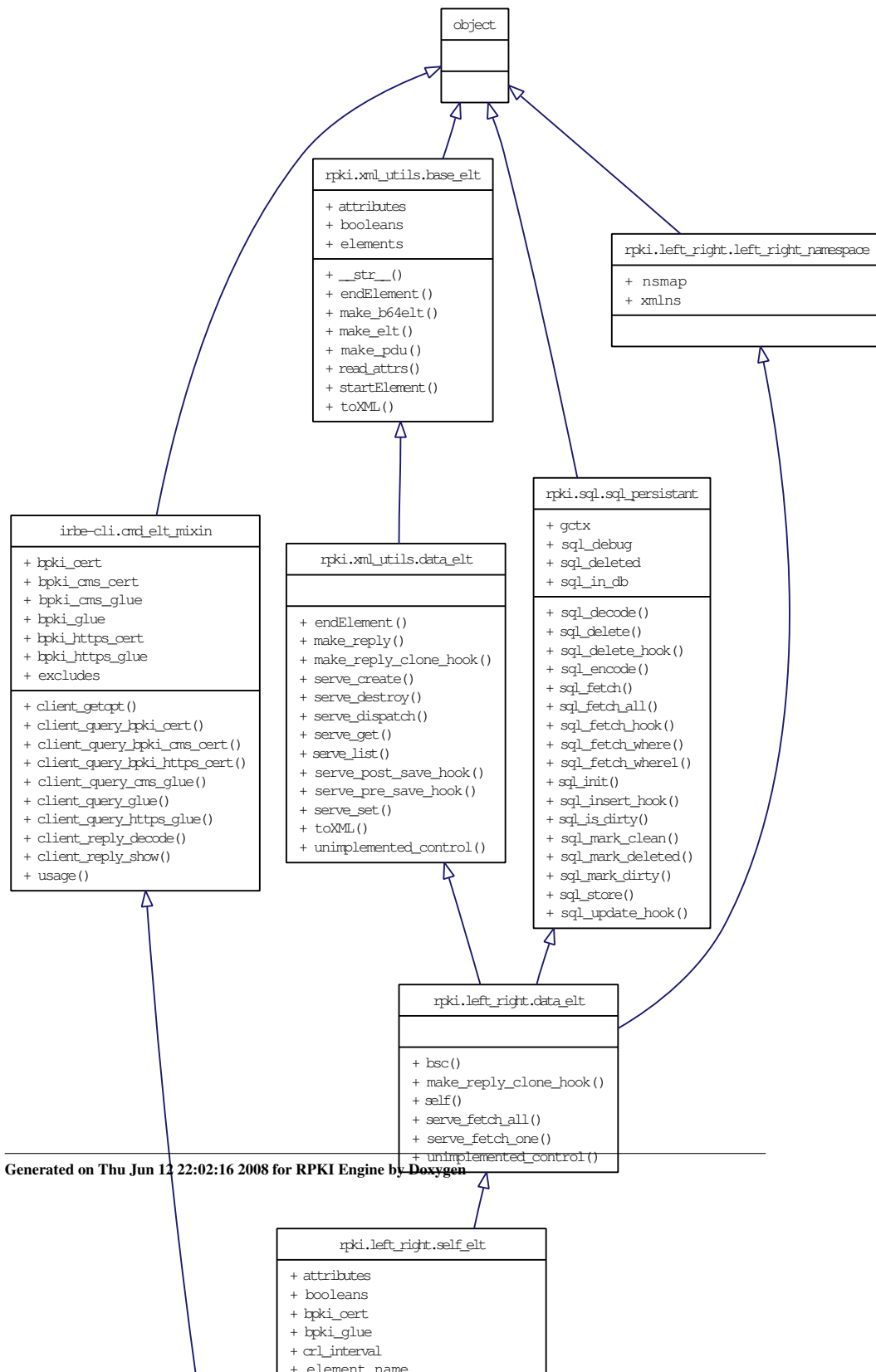
Definition at line 157 of file `irbe-cli.py`.

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

- [irbe-cli.py \(1880\)](#)

7.24 irbe-cli.self_elt Class Reference

Inheritance diagram for irbe-cli.self_elt:



7.24.1 Detailed Description

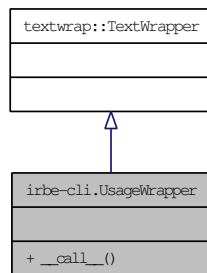
Definition at line 114 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.25 irbe-cli.UsageWrapper Class Reference

Inheritance diagram for irbe-cli.UsageWrapper:



Public Member Functions

- [def `__call__`](#)

7.25.1 Detailed Description

Call interface around Python `textwrap.TextWrapper` class.

Definition at line 26 of file irbe-cli.py.

7.25.2 Member Function Documentation

7.25.2.1 `def irbe-cli.UsageWrapper.__call__(self, args)`

Format arguments, with `TextWrapper` indentation.

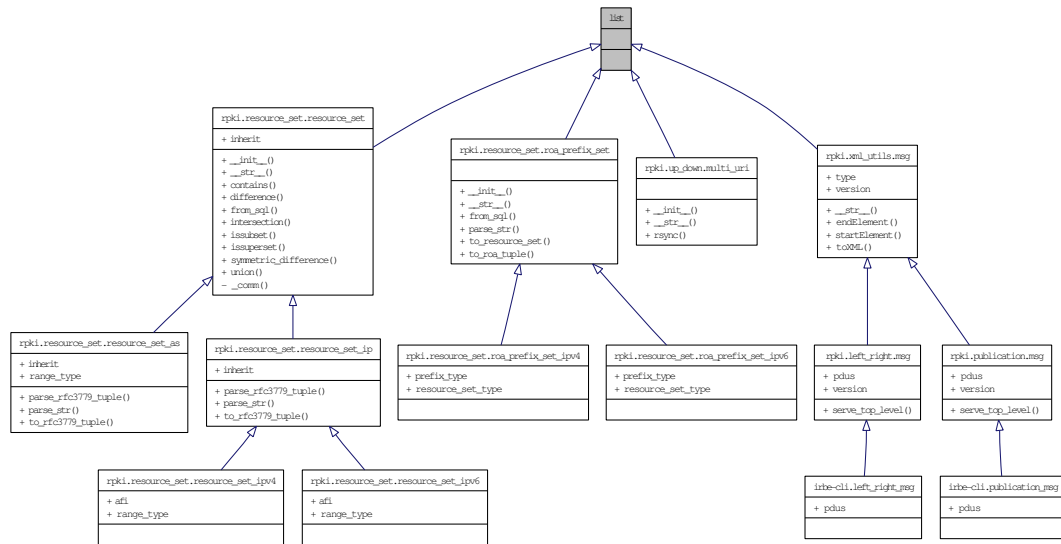
Definition at line 29 of file irbe-cli.py.

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

- [irbe-cli.py \(1880\)](#)

7.26 list Class Reference

Inheritance diagram for list:

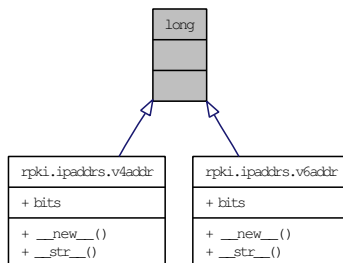


The documentation for this class was generated from the following file:

- [resource_set.py \(1873\)](#)

7.27 long Class Reference

Inheritance diagram for long:

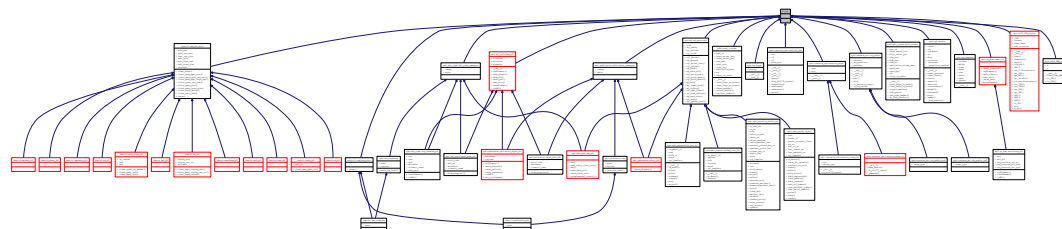


The documentation for this class was generated from the following file:

- [ipaddrs.py \(1873\)](#)

7.28 object Class Reference

Inheritance diagram for object:

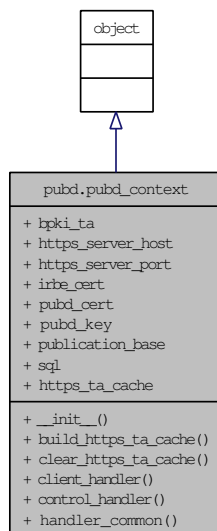


The documentation for this class was generated from the following file:

- [x509.py \(1873\)](#)

7.29 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.

7.29.1 Detailed Description

A container for various pubd parameters.

Definition at line 32 of file pubd.py.

7.29.2 Member Function Documentation

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

Definition at line 35 of file pubd.py.

7.29.2.2 def pubd.pubd_context.build_https_ta_cache (self)

Build dynamic TLS trust anchors.

Definition at line 97 of file pubd.py.

7.29.2.3 def pubd.pubd_context.clear_https_ta_cache (self)

Clear dynamic TLS trust anchors.

Definition at line 90 of file pubd.py.

7.29.2.4 def pubd.pubd_context.client_handler (self, query, path)

Process one PDU from a client.

Definition at line 67 of file pubd.py.

7.29.2.5 def pubd.pubd_context.control_handler (self, query, path)

Process one PDU from the IRBE.

Definition at line 57 of file pubd.py.

7.29.2.6 def pubd.pubd_context.handler_common (self, query, client, certs, crt = None)

Common PDU handler code.

Definition at line 49 of file pubd.py.

7.29.3 Member Data Documentation**7.29.3.1 pubd.pubd_context.bpki_ta**

Definition at line 39 of file pubd.py.

7.29.3.2 pubd.pubd_context.https_server_host

Definition at line 44 of file pubd.py.

7.29.3.3 pubd.pubd_context.https_server_port

Definition at line 45 of file pubd.py.

7.29.3.4 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.

7.29.3.5 pubd.pubd_context.irbe_cert

Definition at line 40 of file pubd.py.

7.29.3.6 pubd.pubd_context.pubd_cert

Definition at line 41 of file pubd.py.

7.29.3.7 pubd.pubd_context.pubd_key

Definition at line 42 of file pubd.py.

7.29.3.8 pubd.pubd_context.publication_base

Definition at line 47 of file pubd.py.

7.29.3.9 pubd.pubd_context.sql

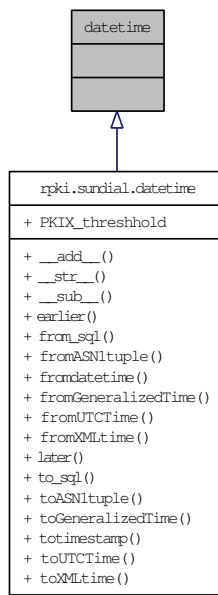
Definition at line 37 of file pubd.py.

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

- [pubd.py \(1880\)](#)

7.30 datetime Class Reference

Inheritance diagram for datetime:

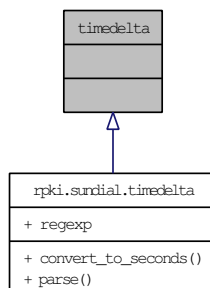


The documentation for this class was generated from the following file:

- [sundial.py \(1873\)](#)

7.31 timedelta Class Reference

Inheritance diagram for timedelta:

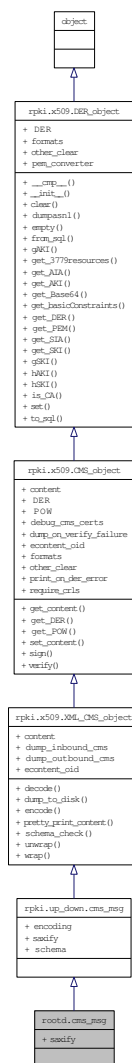


The documentation for this class was generated from the following file:

- [sundial.py \(1873\)](#)

7.32 rootd.cms_msg Class Reference

Inheritance diagram for rootd.cms_msg:



Static Public Attributes

- [saxify](#) = sax_handler.saxify

7.32.1 Detailed Description

Definition at line 130 of file rootd.py.

7.32.2 Member Data Documentation

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

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

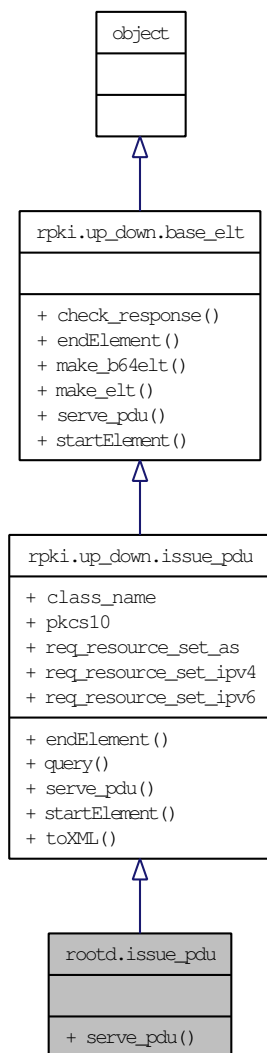
Definition at line 131 of file rootd.py.

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

- [rootd.py](#) (1880)

7.33 rootd.issue_pdu Class Reference

Inheritance diagram for rootd.issue_pdu:



Public Member Functions

- def [serve_pdu](#)

7.33.1 Detailed Description

Definition at line 73 of file rootd.py.

7.33.2 Member Function Documentation

7.33.2.1 def rootd.issue_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*)

Serve one issue request PDU.

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

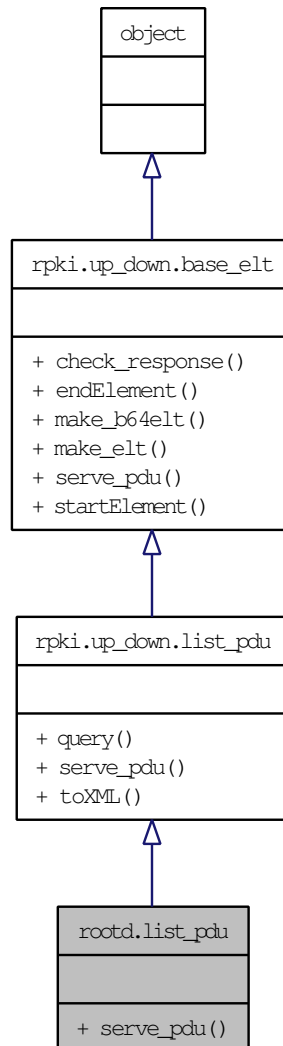
Definition at line 74 of file rootd.py.

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

- [rootd.py](#) (1880)

7.34 rootd.list_pdu Class Reference

Inheritance diagram for rootd.list_pdu:



Public Member Functions

- def [serve_pdu](#)

7.34.1 Detailed Description

Definition at line 68 of file rootd.py.

7.34.2 Member Function Documentation

7.34.2.1 def rootd.list_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*)

Serve one "list" PDU.

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

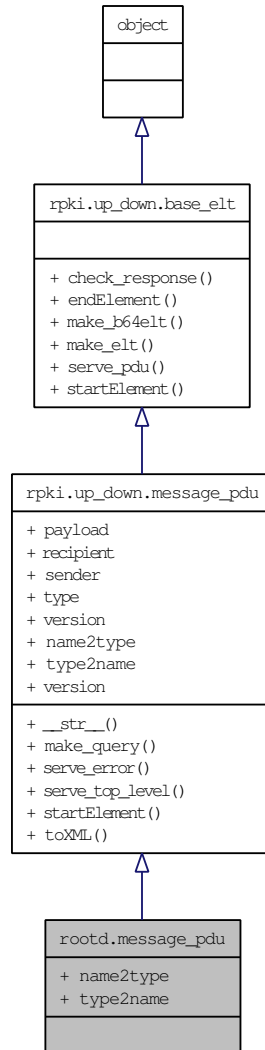
Definition at line 69 of file rootd.py.

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

- [rootd.py \(1880\)](#)

7.35 rootd.message_pdu Class Reference

Inheritance diagram for rootd.message_pdu:



Static Public Attributes

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

7.35.1 Detailed Description

Definition at line 116 of file rootd.py.

7.35.2 Member Data Documentation

7.35.2.1 dictionary rootd.message_pdu.name2type [static]

Initial value:

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

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

Definition at line 117 of file rootd.py.

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

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

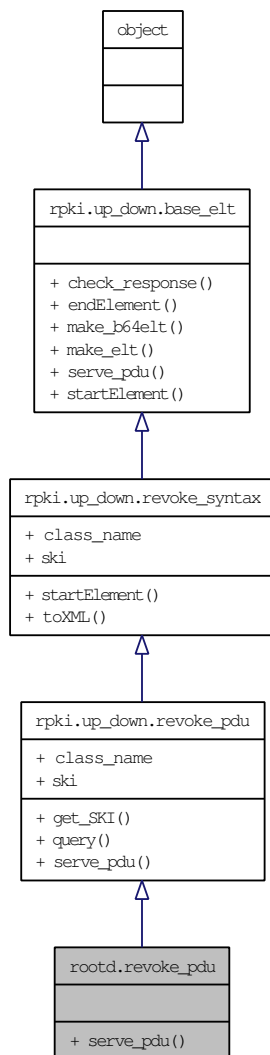
Definition at line 125 of file rootd.py.

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

- [rootd.py \(1880\)](#)

7.36 rootd.revoke_pdu Class Reference

Inheritance diagram for rootd.revoke_pdu:



Public Member Functions

- def [serve_pdu](#)

7.36.1 Detailed Description

Definition at line 106 of file rootd.py.

7.36.2 Member Function Documentation

7.36.2.1 def rootd.revoke_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*)

Serve one revoke request PDU.

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

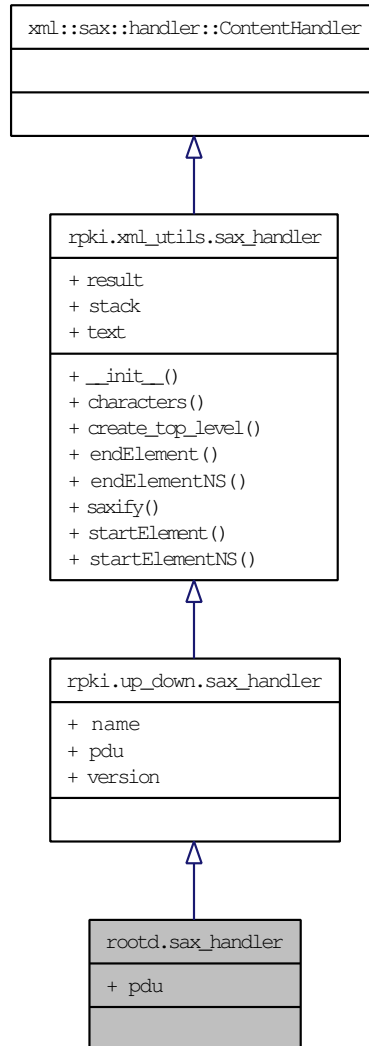
Definition at line 107 of file rootd.py.

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

- [rootd.py \(1880\)](#)

7.37 rootd.sax_handler Class Reference

Inheritance diagram for rootd.sax_handler:



Static Public Attributes

- `pdu` = `message_pdu`

7.37.1 Detailed Description

Definition at line 127 of file rootd.py.

7.37.2 Member Data Documentation

7.37.2.1 rootd.sax_handler.pdu = message_pdu [static]

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

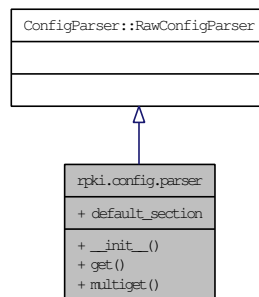
Definition at line 128 of file rootd.py.

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

- [rootd.py \(1880\)](#)

7.38 rpki.config.parser Class Reference

Inheritance diagram for rpki.config.parser:



Public Member Functions

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

Public Attributes

- [default_section](#)

7.38.1 Detailed Description

Definition at line 23 of file config.py.

7.38.2 Member Function Documentation

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

Initialize this parser.

Definition at line 25 of file config.py.

7.38.2.2 `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.

7.38.2.3 `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.

7.38.3 Member Data Documentation

7.38.3.1 `rpki.config.parser.default_section`

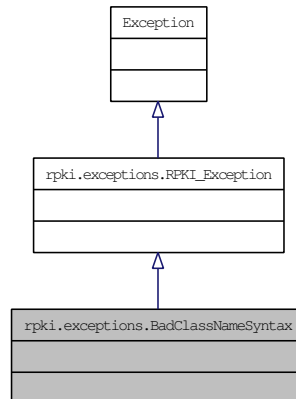
Definition at line 30 of file config.py.

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

- [config.py \(1873\)](#)

7.39 rpki.exceptions.BadClassNameSyntax Class Reference

Inheritance diagram for rpki.exceptions.BadClassNameSyntax:



7.39.1 Detailed Description

Illegal syntax for a class_name.

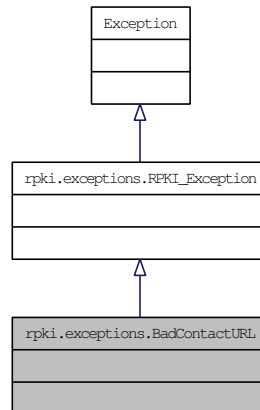
Definition at line 53 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.40 rpki.exceptions.BadContactURL Class Reference

Inheritance diagram for rpki.exceptions.BadContactURL:



7.40.1 Detailed Description

Error trying to parse up-down protocol contact URL.

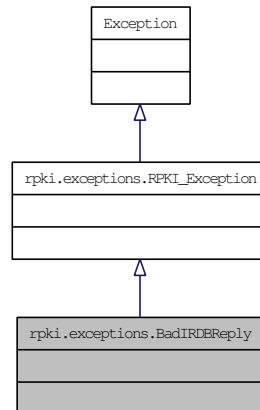
Definition at line 50 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.41 rpki.exceptions.BadIRDBReply Class Reference

Inheritance diagram for rpki.exceptions.BadIRDBReply:



7.41.1 Detailed Description

Unexpected reply to IRDB query.

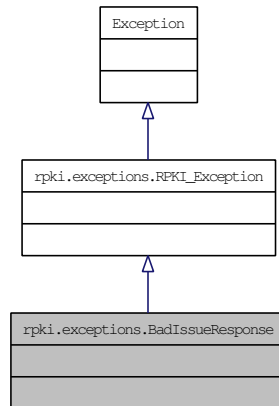
Definition at line 86 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.42 rpki.exceptions.BadIssueResponse Class Reference

Inheritance diagram for rpki.exceptions.BadIssueResponse:



7.42.1 Detailed Description

issue_response PDU with wrong number of classes or certificates.

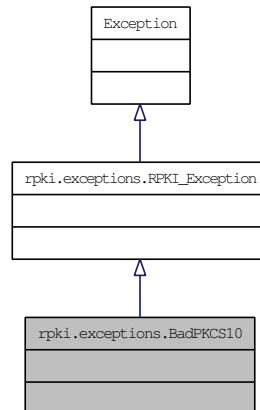
Definition at line 56 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.43 rpki.exceptions.BadPKCS10 Class Reference

Inheritance diagram for rpki.exceptions.BadPKCS10:



7.43.1 Detailed Description

Bad PKCS #10 object.

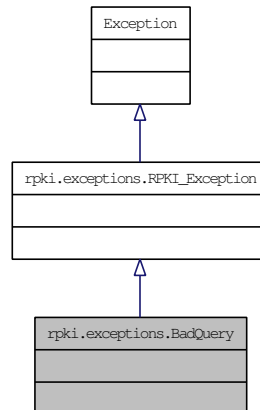
Definition at line 62 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.44 rpki.exceptions.BadQuery Class Reference

Inheritance diagram for rpki.exceptions.BadQuery:



7.44.1 Detailed Description

Unexpected protocol query.

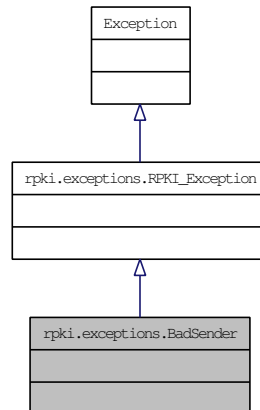
Definition at line 32 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.45 rpki.exceptions.BadSender Class Reference

Inheritance diagram for rpki.exceptions.BadSender:



7.45.1 Detailed Description

Unexpected XML sender value.

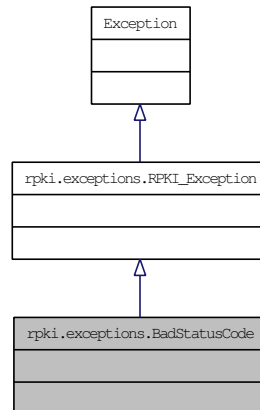
Definition at line 74 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.46 rpki.exceptions.BadStatusCode Class Reference

Inheritance diagram for rpki.exceptions.BadStatusCode:



7.46.1 Detailed Description

Unrecognized protocol status code.

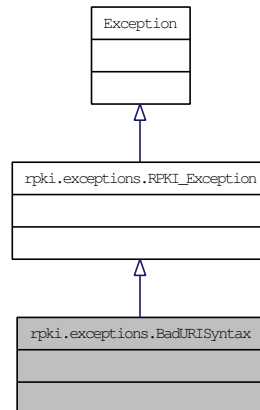
Definition at line 29 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.47 rpki.exceptions.BadURISyntax Class Reference

Inheritance diagram for rpki.exceptions.BadURISyntax:



7.47.1 Detailed Description

Illegal syntax for a URI.

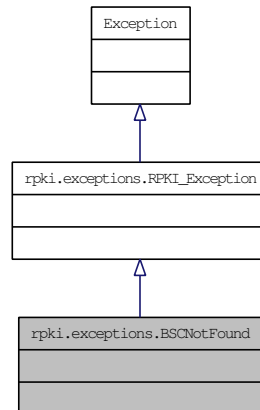
Definition at line 26 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.48 rpki.exceptions.BSCNotFound Class Reference

Inheritance diagram for rpki.exceptions.BSCNotFound:



7.48.1 Detailed Description

Could not find specified BSC in database.

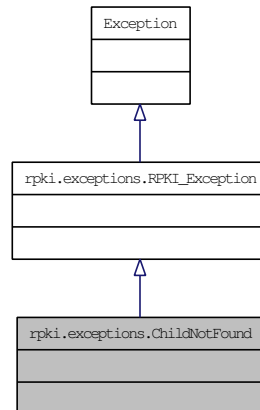
Definition at line 71 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.49 rpki.exceptions.ChildNotFound Class Reference

Inheritance diagram for rpki.exceptions.ChildNotFound:



7.49.1 Detailed Description

Could not find specified child in database.

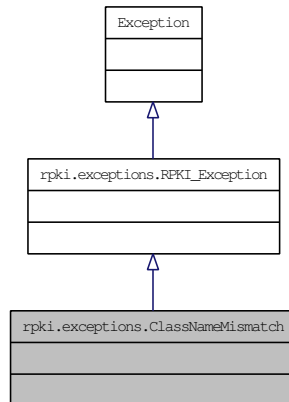
Definition at line 68 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.50 rpki.exceptions.ClassNameMismatch Class Reference

Inheritance diagram for rpki.exceptions.ClassNameMismatch:



7.50.1 Detailed Description

`class_name` does not match child context.

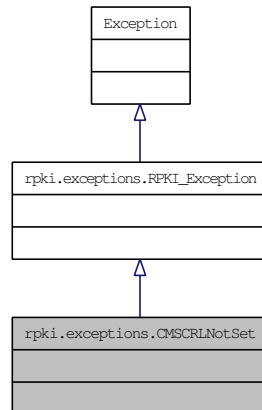
Definition at line 77 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.51 rpki.exceptions.CMSCRLNotSet Class Reference

Inheritance diagram for rpki.exceptions.CMSCRLNotSet:



7.51.1 Detailed Description

CMS CRL has not been configured.

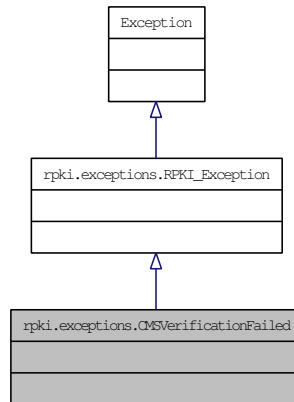
Definition at line 125 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.52 rpki.exceptions.CMSVerificationFailed Class Reference

Inheritance diagram for rpki.exceptions.CMSVerificationFailed:



7.52.1 Detailed Description

Verification of a CMS message failed.

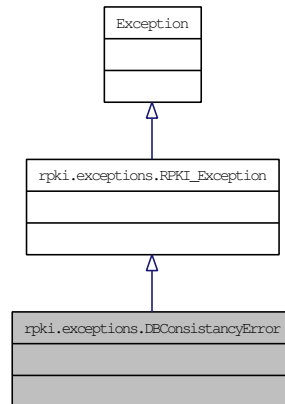
Definition at line 38 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.53 rpki.exceptions.DBConsistencyError Class Reference

Inheritance diagram for rpki.exceptions.DBConsistencyError:



7.53.1 Detailed Description

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

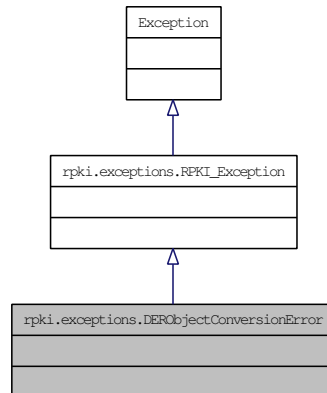
Definition at line 35 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.54 rpki.exceptions.DERObjectConversionError Class Reference

Inheritance diagram for rpki.exceptions.DERObjectConversionError:



7.54.1 Detailed Description

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

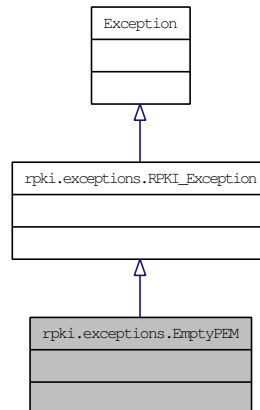
Definition at line 44 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.55 rpki.exceptions.EmptyPEM Class Reference

Inheritance diagram for rpki.exceptions.EmptyPEM:



7.55.1 Detailed Description

Couldn't find PEM block to convert.

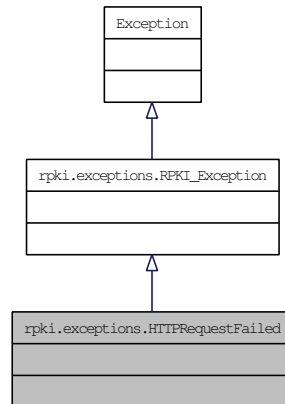
Definition at line 107 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.56 rpki.exceptions.HTTPRequestFailed Class Reference

Inheritance diagram for rpki.exceptions.HTTPRequestFailed:



7.56.1 Detailed Description

HTTP request failed.

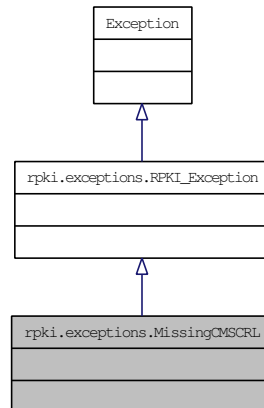
Definition at line 41 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.57 rpki.exceptions.MissingCMSCRL Class Reference

Inheritance diagram for rpki.exceptions.MissingCMSCRL:



7.57.1 Detailed Description

Didn't receive CMS CRL when expecting one.

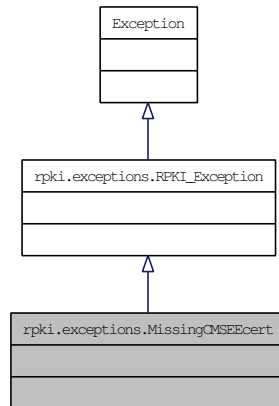
Definition at line 119 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.58 rpki.exceptions.MissingCMSEECert Class Reference

Inheritance diagram for rpki.exceptions.MissingCMSEECert:



7.58.1 Detailed Description

Didn't receive CMS EE cert when expecting one.

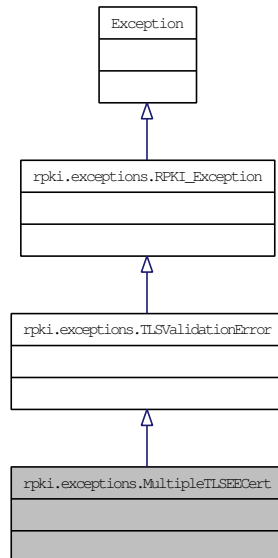
Definition at line 116 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.59 rpki.exceptions.MultipleTLSEECert Class Reference

Inheritance diagram for rpki.exceptions.MultipleTLSEECert:



7.59.1 Detailed Description

Received more than one TLS EE certificate.

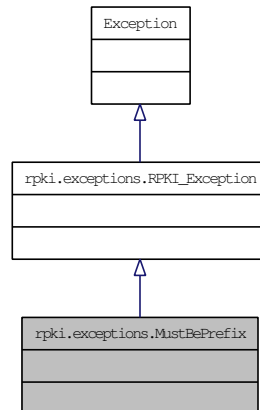
Definition at line 98 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.60 rpki.exceptions.MustBePrefix Class Reference

Inheritance diagram for rpki.exceptions.MustBePrefix:



7.60.1 Detailed Description

Resource range cannot be expressed as a prefix.

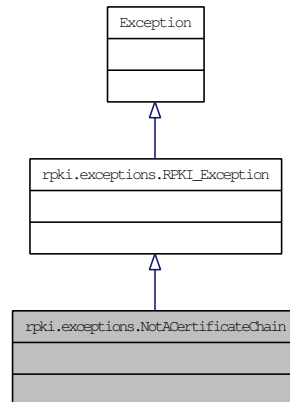
Definition at line 92 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.61 rpki.exceptions.NotACertificateChain Class Reference

Inheritance diagram for rpki.exceptions.NotACertificateChain:



7.61.1 Detailed Description

Certificates don't form a proper chain.

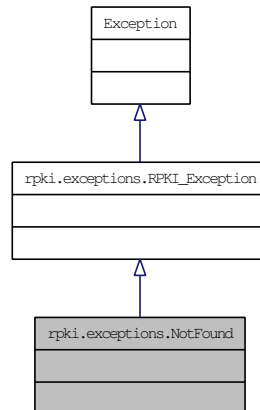
Definition at line 47 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.62 rpki.exceptions.NotFound Class Reference

Inheritance diagram for rpki.exceptions.NotFound:



7.62.1 Detailed Description

Object not found in database.

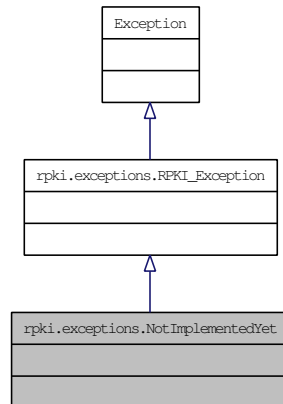
Definition at line 89 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.63 rpki.exceptions.NotImplementedYet Class Reference

Inheritance diagram for rpki.exceptions.NotImplementedYet:



7.63.1 Detailed Description

Internal error -- not implemented yet.

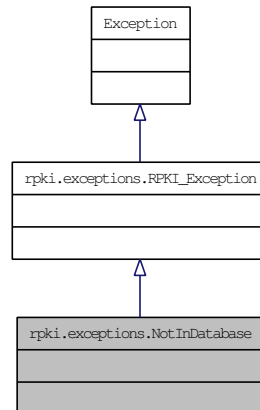
Definition at line 59 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.64 rpki.exceptions.NotInDatabase Class Reference

Inheritance diagram for rpki.exceptions.NotInDatabase:



7.64.1 Detailed Description

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

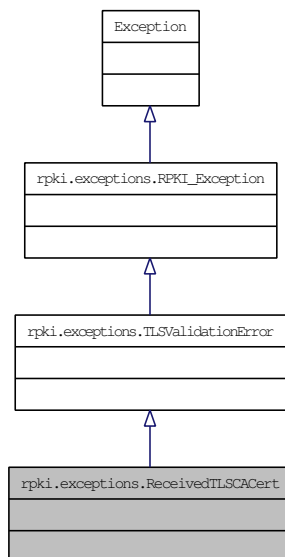
Definition at line 23 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.65 rpki.exceptions.ReceivedTLSCACert Class Reference

Inheritance diagram for rpki.exceptions.ReceivedTLSCACert:



7.65.1 Detailed Description

Received CA certificate via TLS.

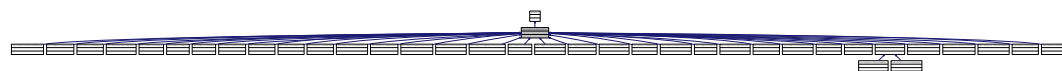
Definition at line 101 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.66 rpki.exceptions.RPKI_Exception Class Reference

Inheritance diagram for rpki.exceptions.RPKI_Exception:



7.66.1 Detailed Description

Base class for RPKI exceptions.

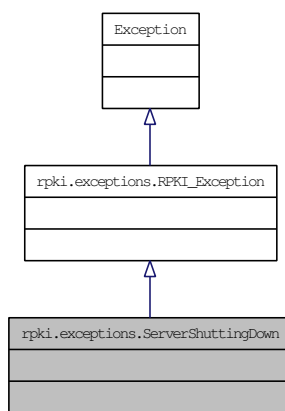
Definition at line 20 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.67 rpki.exceptions.ServerShuttingDown Class Reference

Inheritance diagram for rpki.exceptions.ServerShuttingDown:



7.67.1 Detailed Description

Server is shutting down.

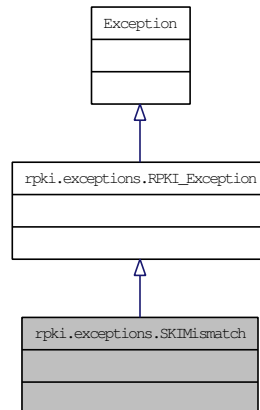
Definition at line 128 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.68 rpki.exceptions.SKIMismatch Class Reference

Inheritance diagram for rpki.exceptions.SKIMismatch:



7.68.1 Detailed Description

SKI value in response does not match request.

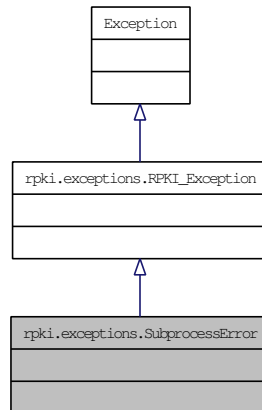
Definition at line 80 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.69 rpki.exceptions.SubprocessError Class Reference

Inheritance diagram for rpki.exceptions.SubprocessError:



7.69.1 Detailed Description

Subprocess returned unexpected error.

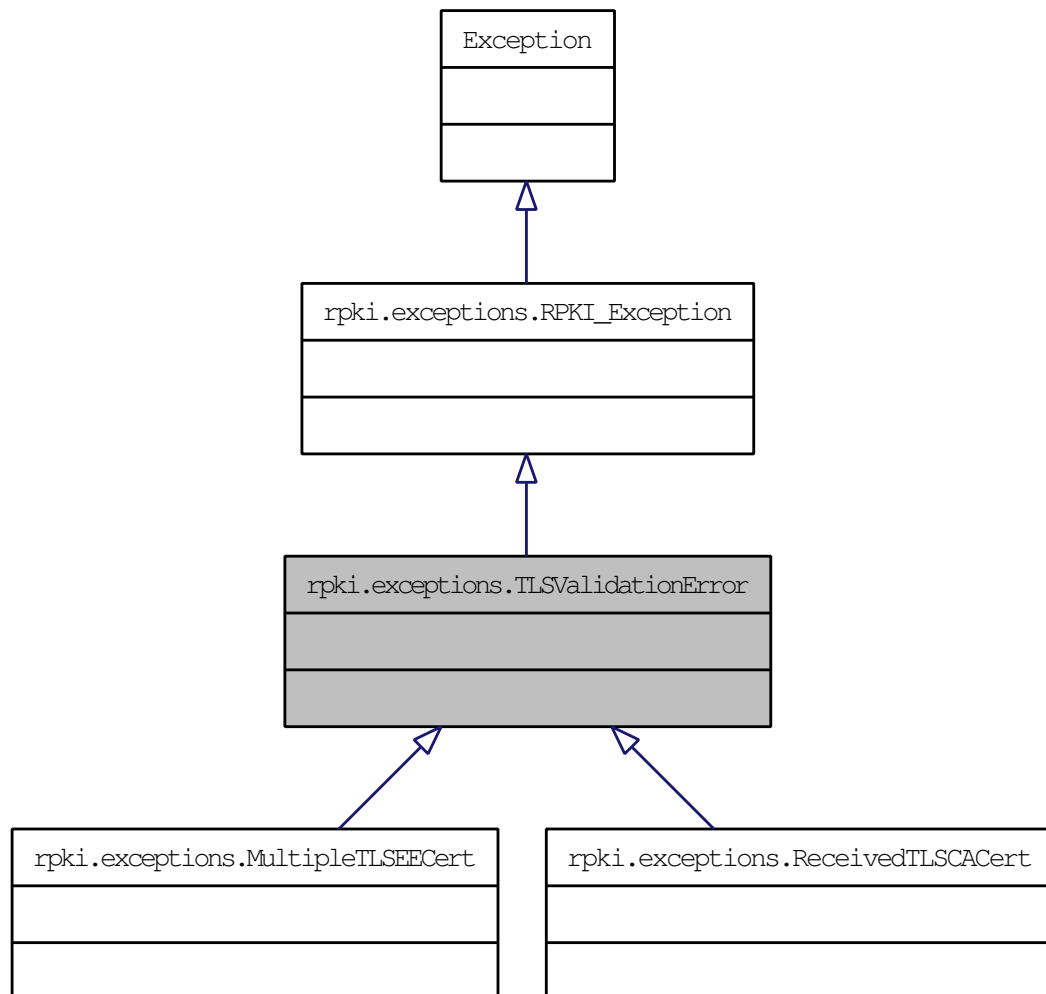
Definition at line 83 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.70 rpki.exceptions.TLSValidationError Class Reference

Inheritance diagram for rpki.exceptions.TLSValidationError:



7.70.1 Detailed Description

TLS certificate validation error.

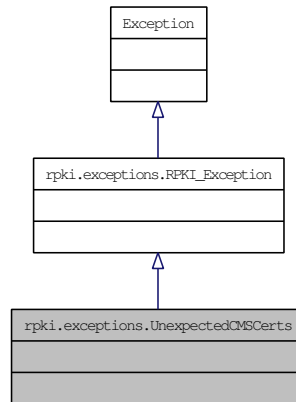
Definition at line 95 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.71 rpki.exceptions.UnexpectedCMSCerts Class Reference

Inheritance diagram for rpki.exceptions.UnexpectedCMSCerts:



7.71.1 Detailed Description

Received CMS certs when not expecting any.

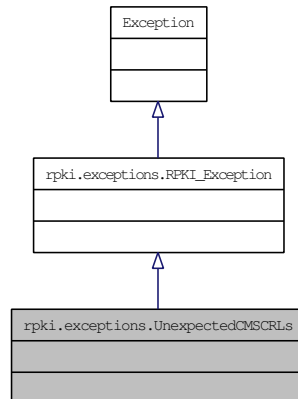
Definition at line 110 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.72 rpki.exceptions.UnexpectedCMSCRLs Class Reference

Inheritance diagram for rpki.exceptions.UnexpectedCMSCRLs:



7.72.1 Detailed Description

Received CMS CRLs when not expecting any.

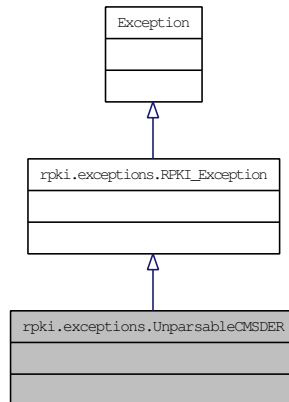
Definition at line 113 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.73 rpki.exceptions.UnparsableCMSDER Class Reference

Inheritance diagram for rpki.exceptions.UnparsableCMSDER:



7.73.1 Detailed Description

Alleged CMS DER wasn't parsable.

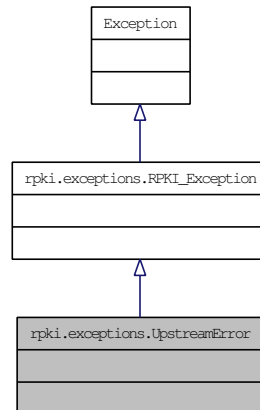
Definition at line 122 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.74 rpki.exceptions.UpstreamError Class Reference

Inheritance diagram for rpki.exceptions.UpstreamError:



7.74.1 Detailed Description

Received an error from upstream.

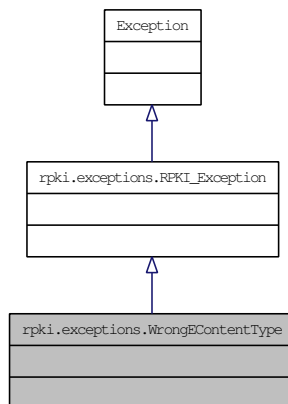
Definition at line 65 of file `exceptions.py`.

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

- [exceptions.py \(1873\)](#)

7.75 rpki.exceptions.WrongEContentType Class Reference

Inheritance diagram for rpki.exceptions.WrongEContentType:



7.75.1 Detailed Description

Received wrong CMS eContentType.

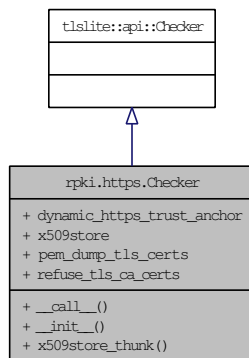
Definition at line 104 of file exceptions.py.

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

- [exceptions.py \(1873\)](#)

7.76 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.

7.76.1 Detailed Description

Derived class to handle X.509 client certificate checking.

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

7.76.2 Member Function Documentation

7.76.2.1 `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`.

7.76.2.2 `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`.

7.76.2.3 def rpki.https.Checker.x509store_thunk (self)

Definition at line 89 of file https.py.

7.76.3 Member Data Documentation

7.76.3.1 rpki.https.Checker.dynamic_https_trust_anchor

Definition at line 72 of file https.py.

7.76.3.2 rpki.https.Checker::pem_dump_tls_certs = False [static]

Vile debugging hack.

Definition at line 67 of file https.py.

7.76.3.3 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.

7.76.3.4 rpki.https.Checker.x509store

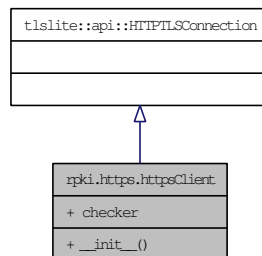
Definition at line 77 of file https.py.

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

- [https.py \(1873\)](#)

7.77 rpki.https.httpsClient Class Reference

Inheritance diagram for rpki.https.httpsClient:



Public Member Functions

- [def __init__](#)

Public Attributes

- [checker](#)

7.77.1 Detailed Description

Derived class to let us replace the default Checker.

Definition at line 138 of file https.py.

7.77.2 Member Function Documentation

7.77.2.1 `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.

7.77.3 Member Data Documentation

7.77.3.1 rpki.https.httpsClient.checker

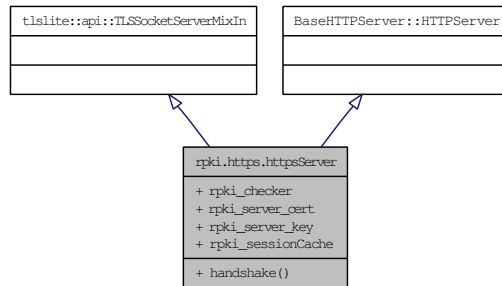
Definition at line 148 of file https.py.

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

- [https.py \(1873\)](#)

7.78 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

7.78.1 Detailed Description

Derived type to handle TLS aspects of HTTPS.

Definition at line 235 of file https.py.

7.78.2 Member Function Documentation

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

TLS handshake handler.

Definition at line 243 of file https.py.

7.78.3 Member Data Documentation

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

Definition at line 241 of file https.py.

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

Definition at line 240 of file https.py.

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

Definition at line 239 of file https.py.

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

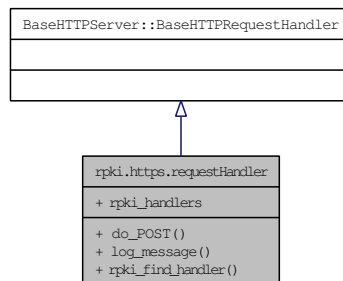
Definition at line 238 of file https.py.

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

- [https.py \(1873\)](#)

7.79 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

7.79.1 Detailed Description

Derived type to supply POST handler and override logging.

Definition at line 196 of file `https.py`.

7.79.2 Member Function Documentation

7.79.2.1 `def rpki.https.requestHandler.do_POST (self)`

POST handler.

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

7.79.2.2 `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`.

7.79.2.3 `def rpki.https.requestHandler.rpki_find_handler (self)`

Helper method to search `self.rpki_handlers`.

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

7.79.3 Member Data Documentation

7.79.3.1 `rpki.https.requestHandler.rpki_handlers = None` [static]

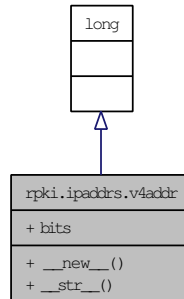
Definition at line 199 of file `https.py`.

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

- [https.py \(1873\)](#)

7.80 rpki.ipaddrs.v4addr Class Reference

Inheritance diagram for rpki.ipaddrs.v4addr:



Public Member Functions

- def [__new__](#)
- def [__str__](#)

Static Public Attributes

- int [bits](#) = 32

7.80.1 Detailed Description

IPv4 address.

Derived from long, but supports IPv4 print syntax.

Definition at line 32 of file ipaddrs.py.

7.80.2 Member Function Documentation

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

Construct a v4addr object.

Definition at line 40 of file ipaddrs.py.

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

Convert a v4addr object to string format.

Definition at line 48 of file ipaddrs.py.

7.80.3 Member Data Documentation

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

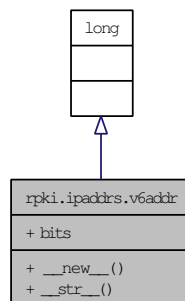
Definition at line 38 of file ipaddrs.py.

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

- [ipaddrs.py \(1873\)](#)

7.81 rpki.ipaddrs.v6addr Class Reference

Inheritance diagram for rpki.ipaddrs.v6addr:



Public Member Functions

- def [__new__](#)
- def [__str__](#)

Static Public Attributes

- int [bits](#) = 128

7.81.1 Detailed Description

IPv6 address.

Derived from long, but supports IPv6 print syntax.

Definition at line 52 of file ipaddrs.py.

7.81.2 Member Function Documentation

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

Construct a v6addr object.

Definition at line 60 of file ipaddrs.py.

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

Convert a v6addr object to string format.

Definition at line 67 of file ipaddrs.py.

7.81.3 Member Data Documentation

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

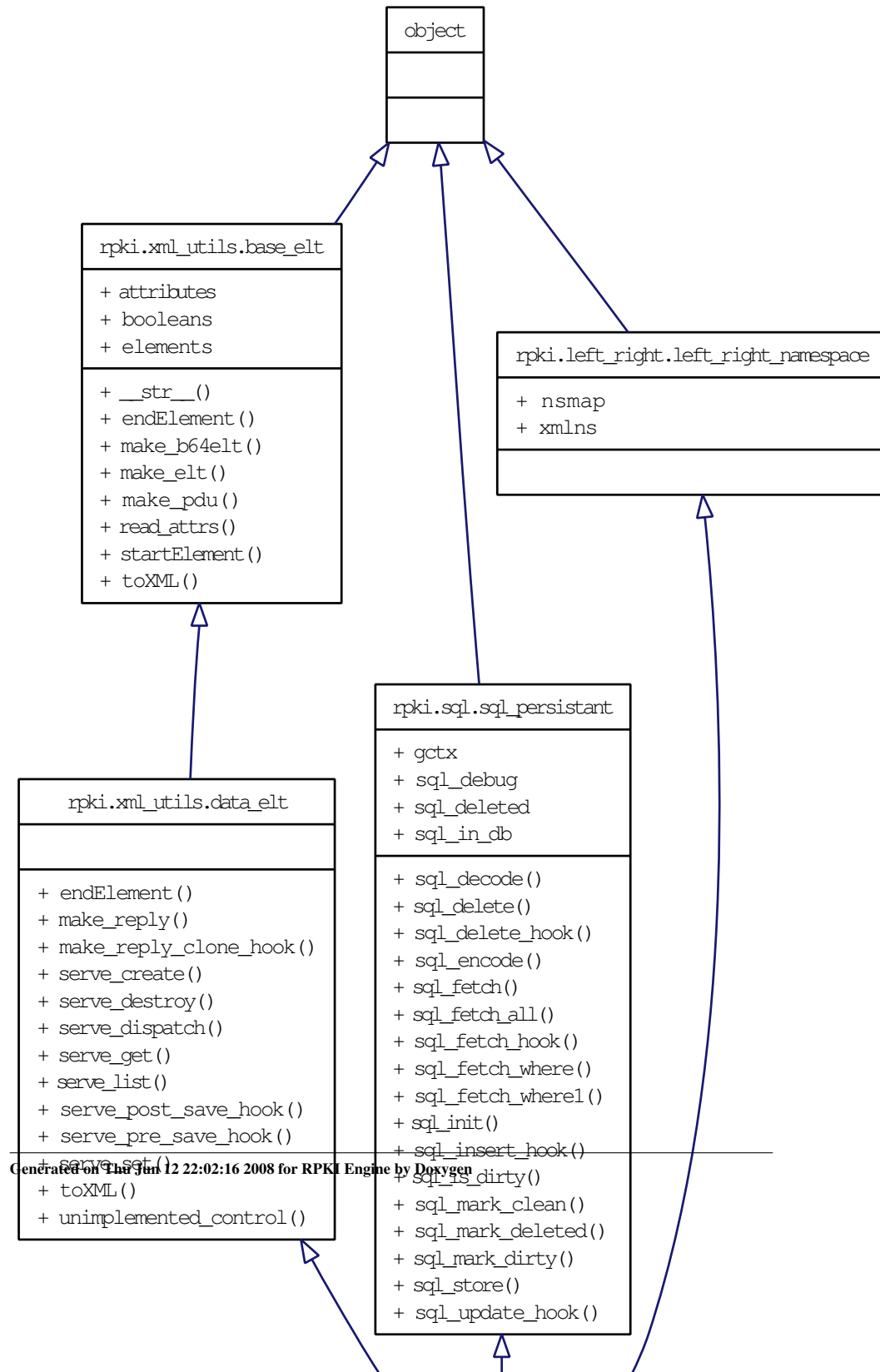
Definition at line 58 of file ipaddrs.py.

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

- [ipaddrs.py \(1873\)](#)

7.82 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](#)

7.82.1 Detailed Description

<bsc/> (Business Signing Context) element.

Definition at line 235 of file left_right.py.

7.82.2 Member Function Documentation

7.82.2.1 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.

7.82.2.2 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.

7.82.2.3 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.

7.82.2.4 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.

7.82.3 Member Data Documentation

7.82.3.1 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.

7.82.3.2 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.

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

Definition at line 238 of file left_right.py.

7.82.3.4 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.

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

Definition at line 250 of file left_right.py.

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

Definition at line 249 of file left_right.py.

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

Reimplemented in [irbe-cli.bsc_elt](#).

Definition at line 251 of file left_right.py.

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

Reimplemented in [irbe-cli.bsc_elt](#).

Definition at line 252 of file left_right.py.

7.82.3.9 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))
```

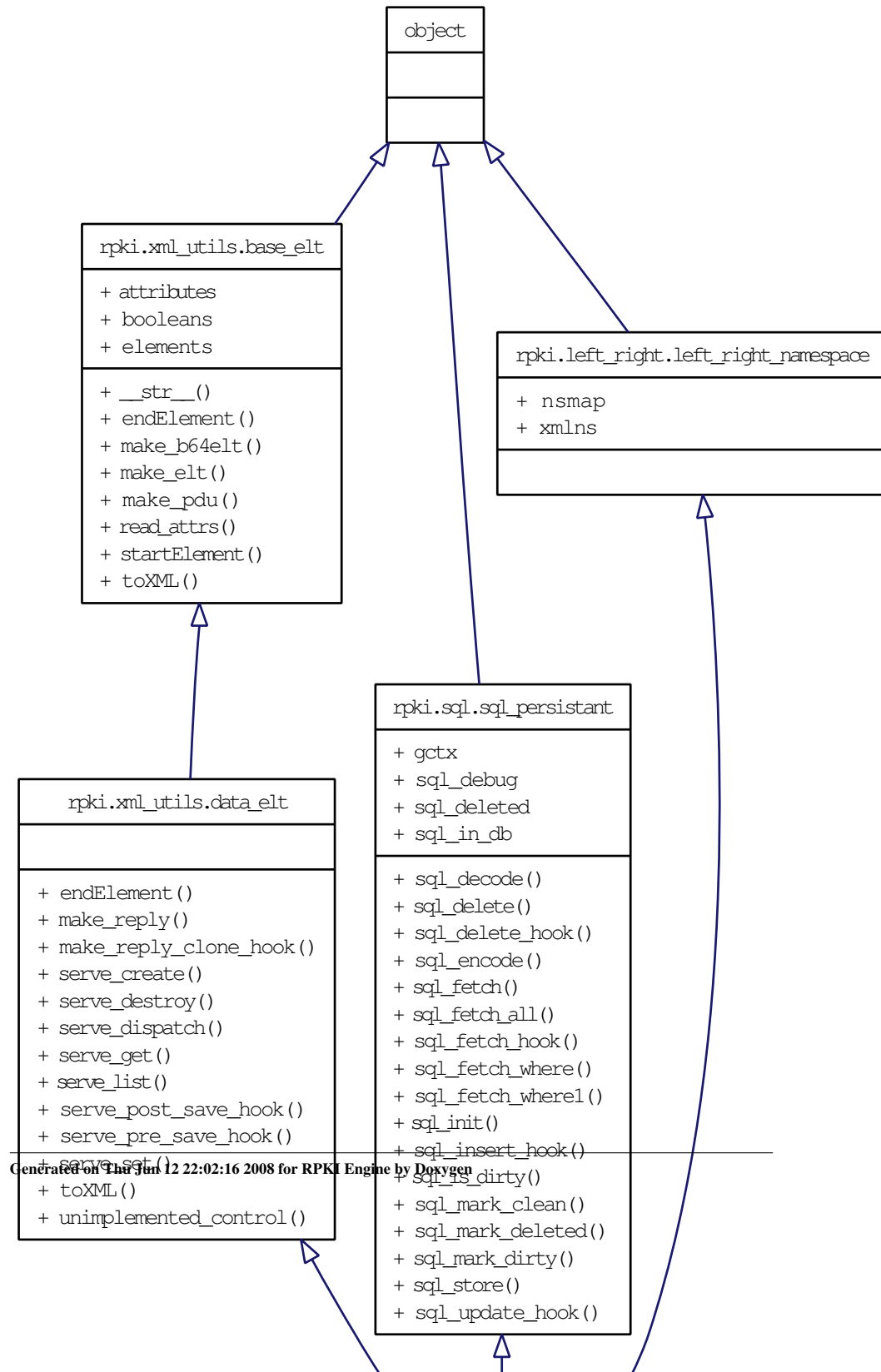
Definition at line 243 of file left_right.py.

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

- [left_right.py](#) (1873)

7.83 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](#)

7.83.1 Detailed Description

<child/> element.

Definition at line 368 of file left_right.py.

7.83.2 Member Function Documentation

7.83.2.1 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.

7.83.2.2 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.

7.83.2.3 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.

7.83.2.4 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.

7.83.2.5 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.

7.83.2.6 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.

7.83.3 Member Data Documentation

7.83.3.1 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.

7.83.3.2 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.

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

Definition at line 380 of file left_right.py.

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

Definition at line 381 of file left_right.py.

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

Definition at line 382 of file left_right.py.

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

Definition at line 371 of file left_right.py.

7.83.3.7 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.

7.83.3.8 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))
```

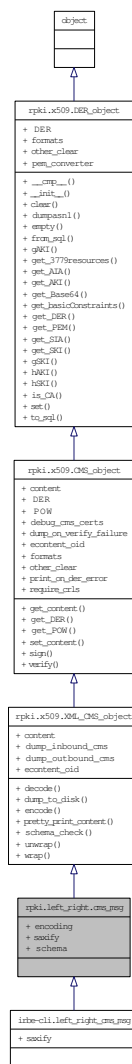
Definition at line 376 of file left_right.py.

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

- [left_right.py \(1873\)](#)

7.84 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`

7.84.1 Detailed Description

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

Definition at line 813 of file left_right.py.

7.84.2 Member Data Documentation

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

Definition at line 816 of file left_right.py.

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

Reimplemented in [irbe-cli.left_right.cms_msg](#).

Definition at line 818 of file left_right.py.

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

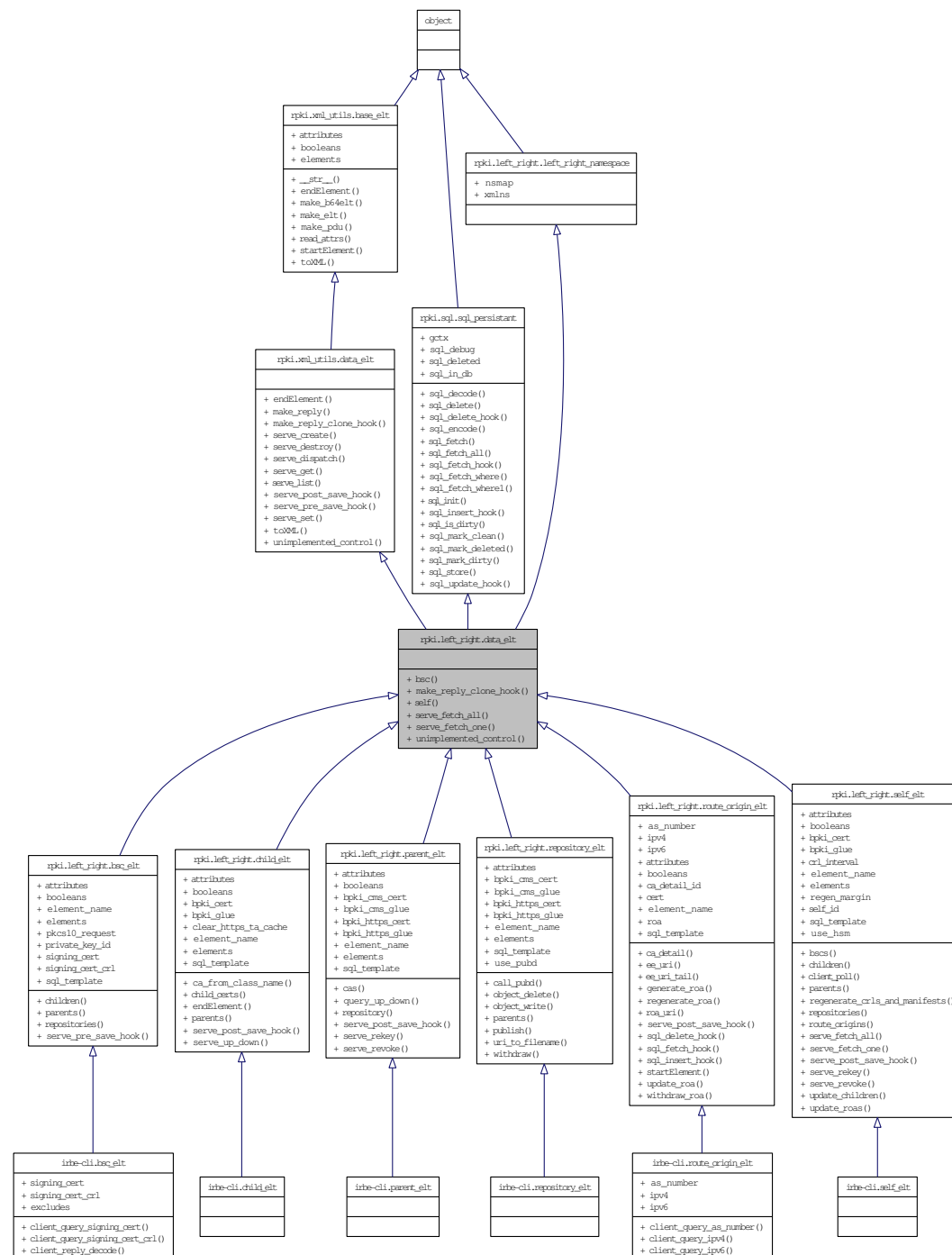
Definition at line 817 of file left_right.py.

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

- [left_right.py](#) (1873)

7.85 rpki.left_right.data_elt Class Reference

Inheritance diagram for rpki.left_right.data_elt:



Generated on Thu Jun 12 22:02:16 2008 for RPKI Engine by Doxygen

Public Member Functions

- def [bsc](#)
- def [make_reply_clone_hook](#)
- def [self](#)
- def [serve_fetch_all](#)
- def [serve_fetch_one](#)
- def [unimplemented_control](#)

7.85.1 Detailed Description

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

Definition at line 34 of file `left_right.py`.

7.85.2 Member Function Documentation

7.85.2.1 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`.

7.85.2.2 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`.

7.85.2.3 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`.

7.85.2.4 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`.

7.85.2.5 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.

7.85.2.6 def rpki.left_right.data_elt.unimplemented_control (self, controls)

Uniform handling for unimplemented control operations.

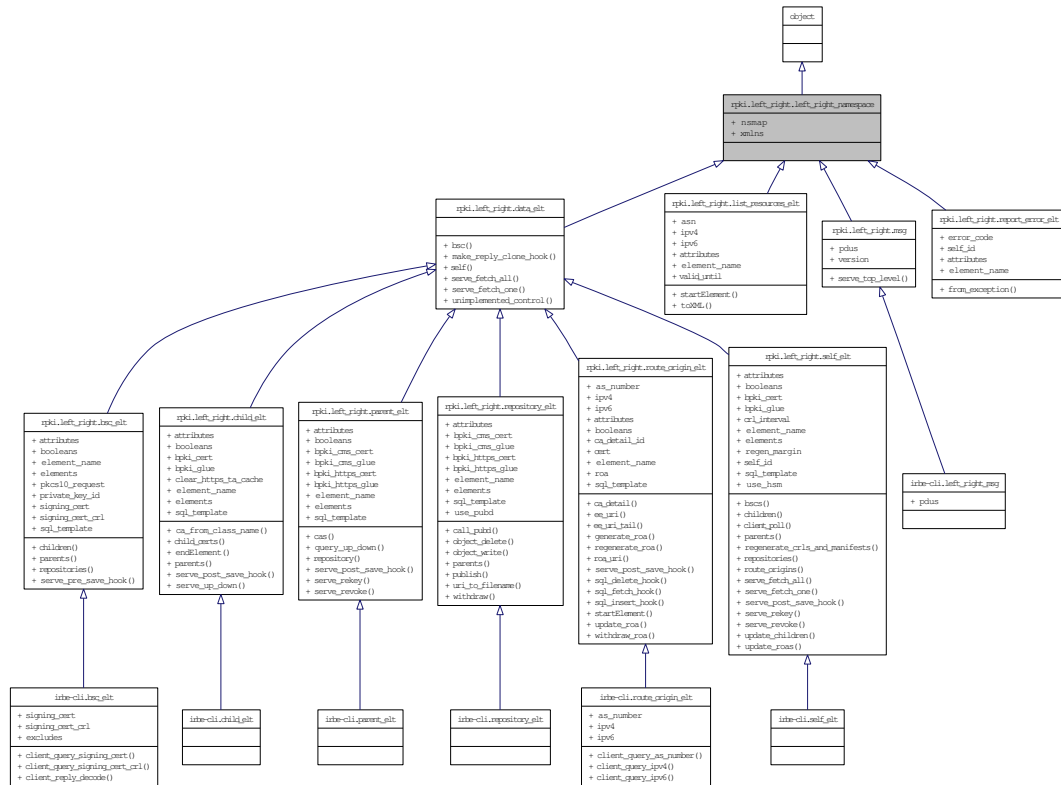
Reimplemented from [rpki.xml_utils.data_elt](#).

Definition at line 64 of file left_right.py.

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

- [left_right.py](#) (1873)

Inheritance diagram for `rpki.left_right.left_right_namespace`:



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

XML namespace parameters for left-right protocol.

Definition at line 28 of file left_right.py.

7.86.2 Member Data Documentation

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

Definition at line 32 of file `left_right.py`.

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

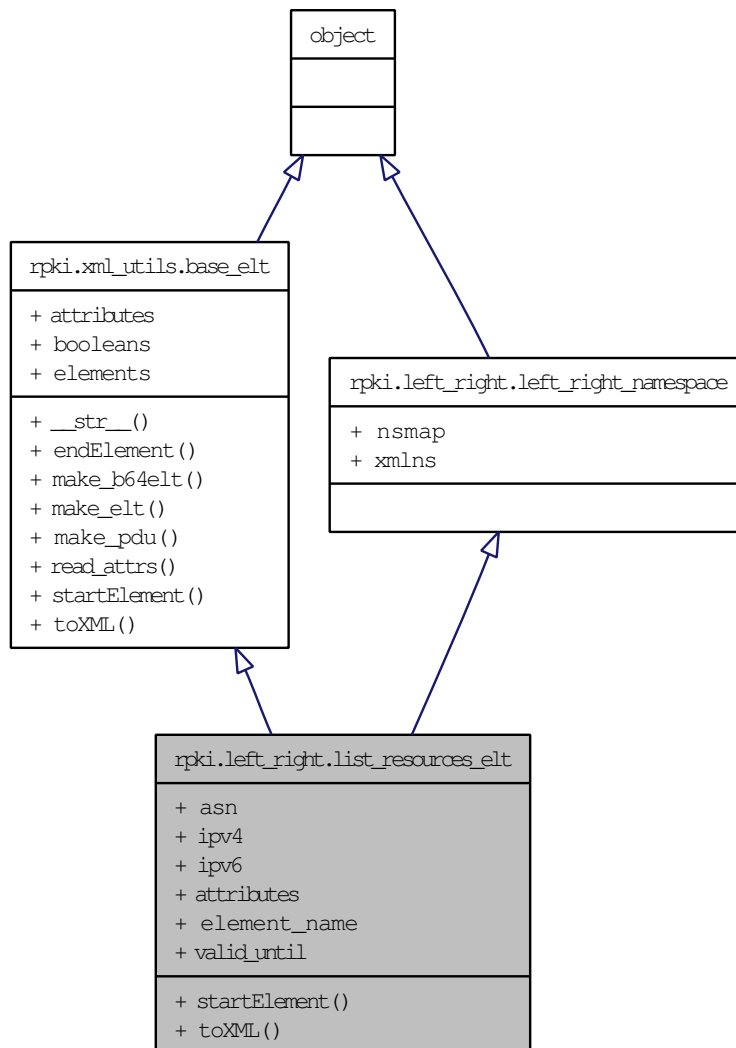
Definition at line 31 of file `left_right.py`.

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

- [left_right.py \(1873\)](#)

7.87 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

7.87.1 Detailed Description

`<list_resources/>` element.

Definition at line 739 of file `left_right.py`.

7.87.2 Member Function Documentation

7.87.2.1 `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`.

7.87.2.2 `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`.

7.87.3 Member Data Documentation

7.87.3.1 rpki.left_right.list_resources_elt.asn

Definition at line 755 of file left_right.py.

7.87.3.2 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.

7.87.3.3 string rpki.left_right.list_resources_elt.element_name = "list-resources" [static]

Definition at line 742 of file left_right.py.

7.87.3.4 rpki.left_right.list_resources_elt.ipv4

Definition at line 757 of file left_right.py.

7.87.3.5 rpki.left_right.list_resources_elt.ipv6

Definition at line 759 of file left_right.py.

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

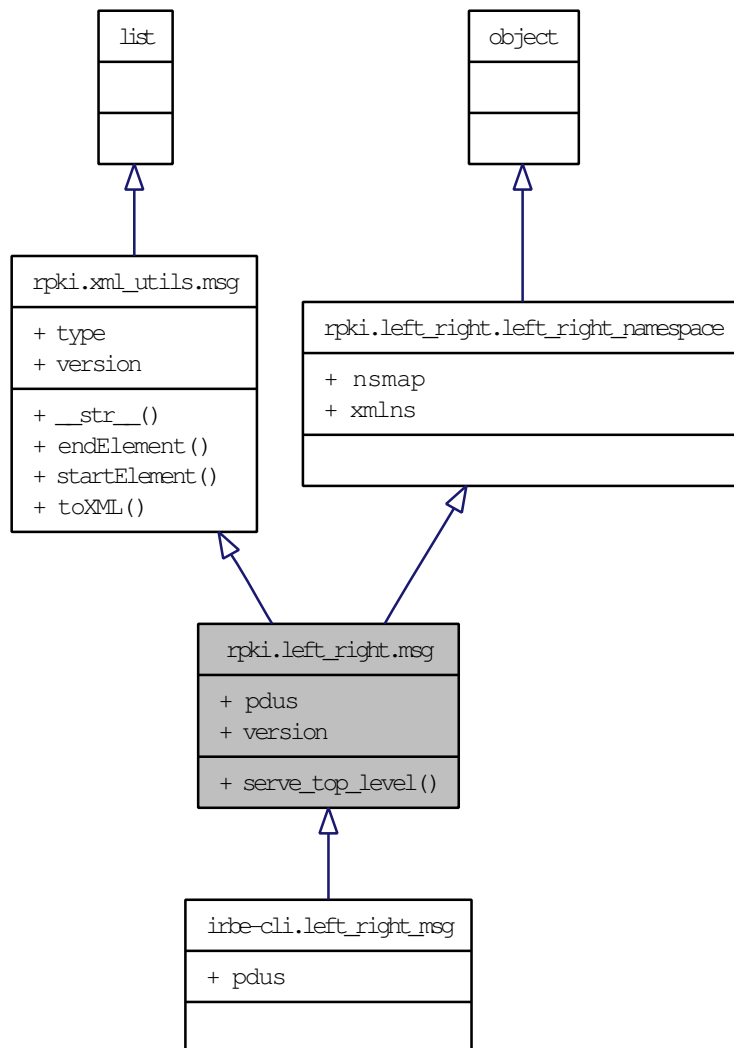
Definition at line 744 of file left_right.py.

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

- [left_right.py](#) (1873)

7.88 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.

7.88.1 Detailed Description

Left-right PDU.

Definition at line 784 of file left_right.py.

7.88.2 Member Function Documentation

7.88.2.1 def rpki.left_right.msg.serve_top_level (self, gctx)

Serve one msg PDU.

Definition at line 797 of file left_right.py.

7.88.3 Member Data Documentation

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

Initial value:

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

Dispatch table of PDUs for this protocol.

Reimplemented in [irbe-cli.left_right_msg](#).

Definition at line 793 of file left_right.py.

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

Protocol version.

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

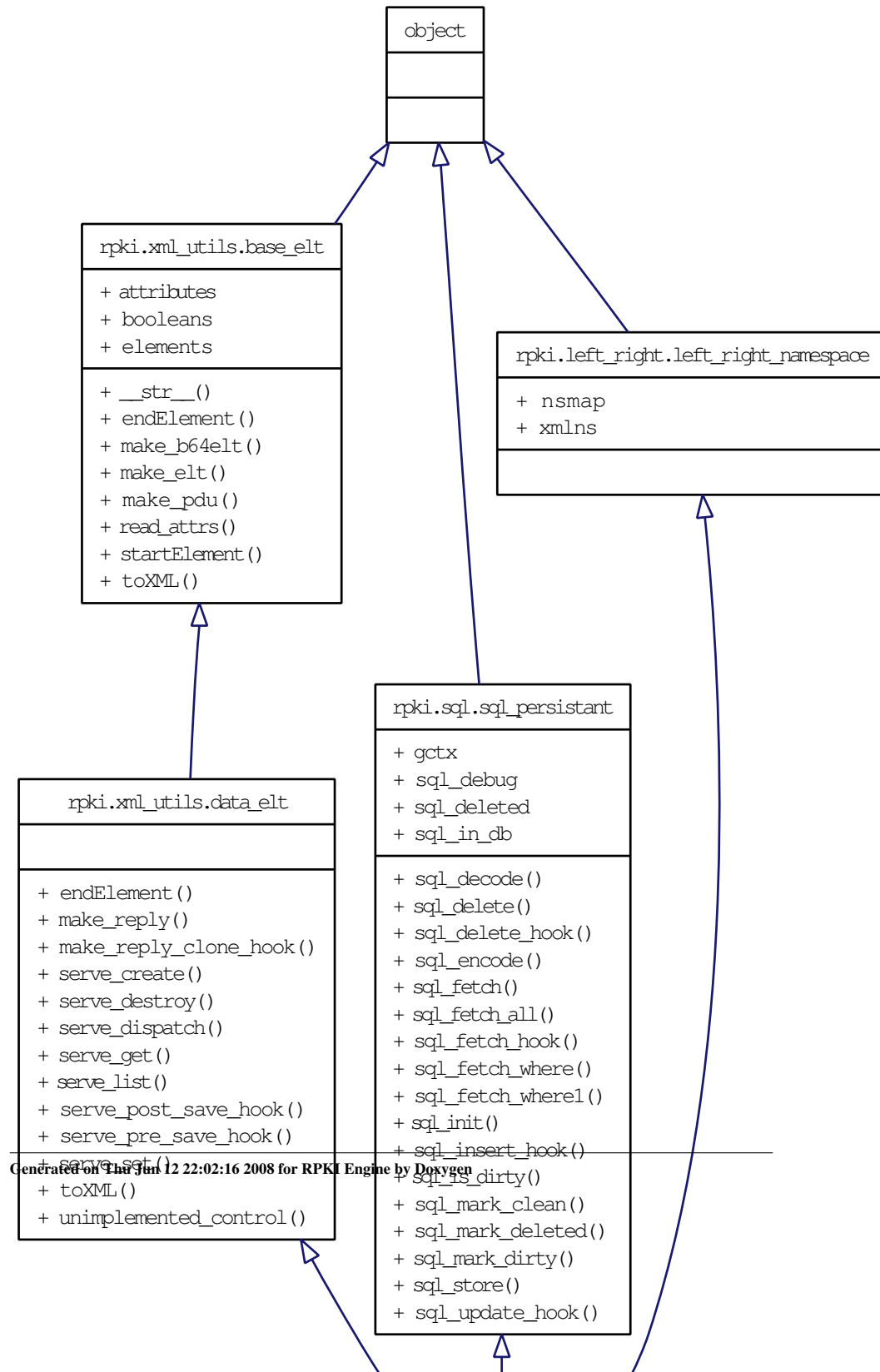
Definition at line 789 of file left_right.py.

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

- [left_right.py \(1873\)](#)

7.89 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](#)

7.89.1 Detailed Description

`<parent/>` element.

Definition at line 278 of file `left_right.py`.

7.89.2 Member Function Documentation

7.89.2.1 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`.

7.89.2.2 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.

7.89.2.3 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.

7.89.2.4 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.

7.89.2.5 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.

7.89.2.6 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.

7.89.3 Member Data Documentation

7.89.3.1 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.

7.89.3.2 tuple rpki.left_right.parent_elt.booleans = ("rekey", "reissue", "re- voke") [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.

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

Definition at line 292 of file left_right.py.

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

Definition at line 293 of file left_right.py.

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

Definition at line 294 of file left_right.py.

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

Definition at line 295 of file left_right.py.

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

Definition at line 281 of file left_right.py.

7.89.3.8 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`.

7.89.3.9 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.X509),
                  ("bpki_https_cert", rpki.x509.X509), ("bpki_https_glue", rpki.x509.X509),
                  "peer_contact_uri", "sia_base", "sender_name", "recipient_name")
```

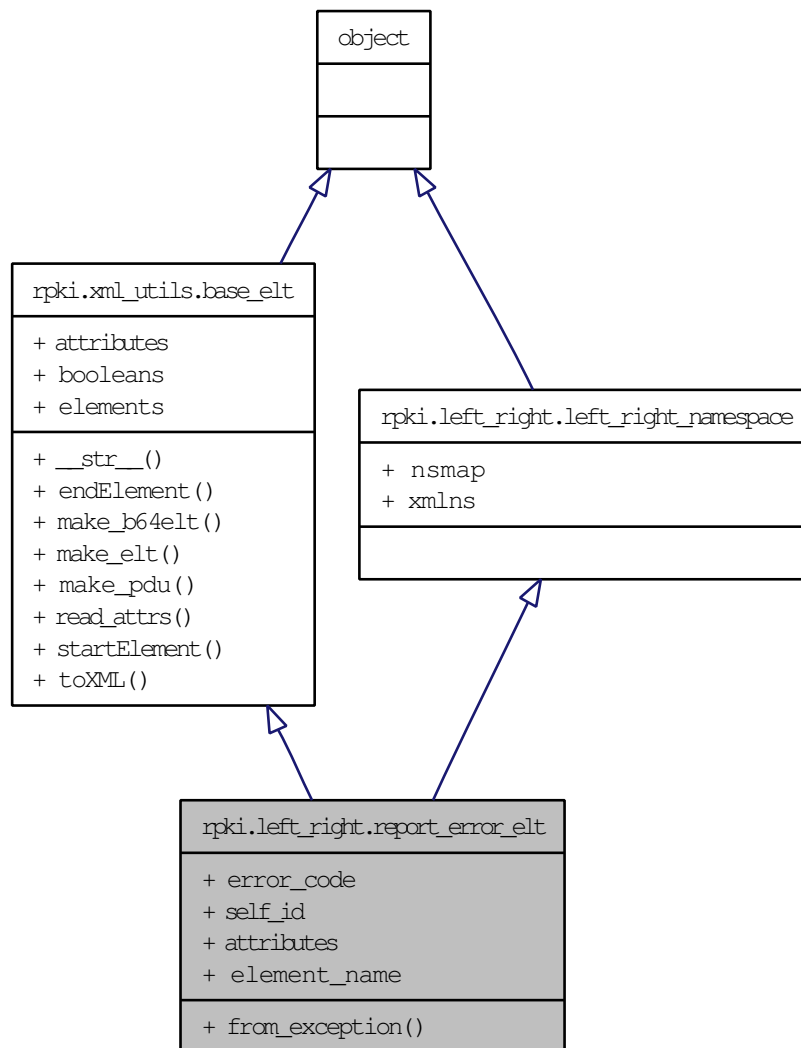
Definition at line 287 of file `left_right.py`.

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

- [left_right.py \(1873\)](#)

7.90 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"

7.90.1 Detailed Description

<report_error/> element.

Definition at line 770 of file left_right.py.

7.90.2 Member Function Documentation

7.90.2.1 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.

7.90.3 Member Data Documentation

7.90.3.1 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.

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

Definition at line 773 of file left_right.py.

7.90.3.3 `rpki.left_right.report_error_elt.error_code`

Definition at line 781 of file `left_right.py`.

7.90.3.4 `rpki.left_right.report_error_elt.self_id`

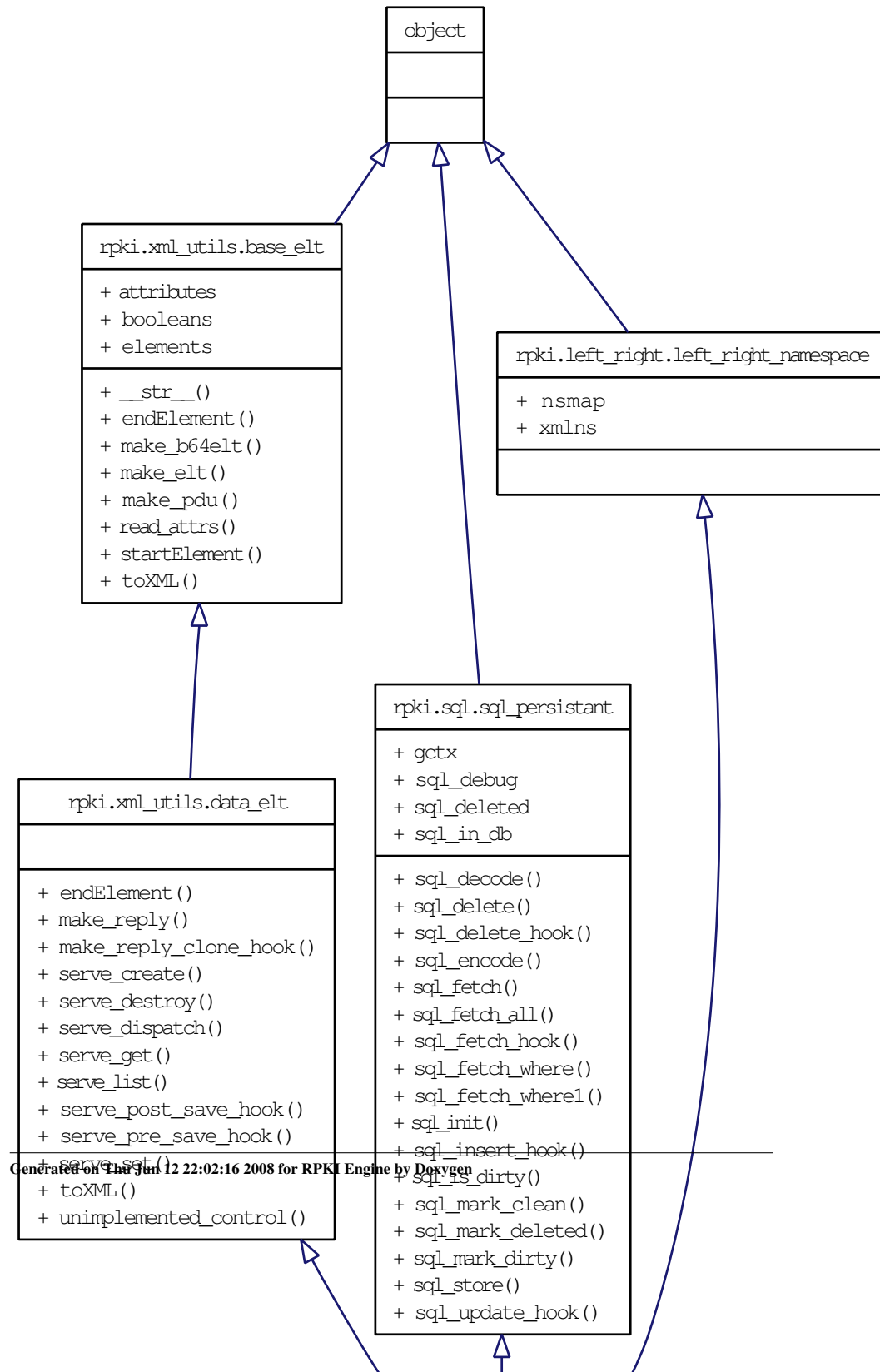
Definition at line 780 of file `left_right.py`.

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

- [left_right.py \(1873\)](#)

7.91 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

7.91.1 Detailed Description

<repository/> element.

Definition at line 446 of file left_right.py.

7.91.2 Member Function Documentation

7.91.2.1 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.

7.91.2.2 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.

7.91.2.3 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.

7.91.2.4 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.

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

Placeholder for publication operation. [TEMPORARY]

Definition at line 514 of file left_right.py.

7.91.2.6 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.

7.91.2.7 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.

7.91.3 Member Data Documentation**7.91.3.1 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.

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

Definition at line 457 of file left_right.py.

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

Definition at line 458 of file left_right.py.

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

Definition at line 459 of file left_right.py.

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

Definition at line 460 of file left_right.py.

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

Definition at line 449 of file left_right.py.

**7.91.3.7 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.

7.91.3.8 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.X509),  
                  ("bpki_https_cert", rpki.x509.X509), ("bpki_https_glue", rpki.x509.X509))
```

Definition at line 453 of file left_right.py.

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

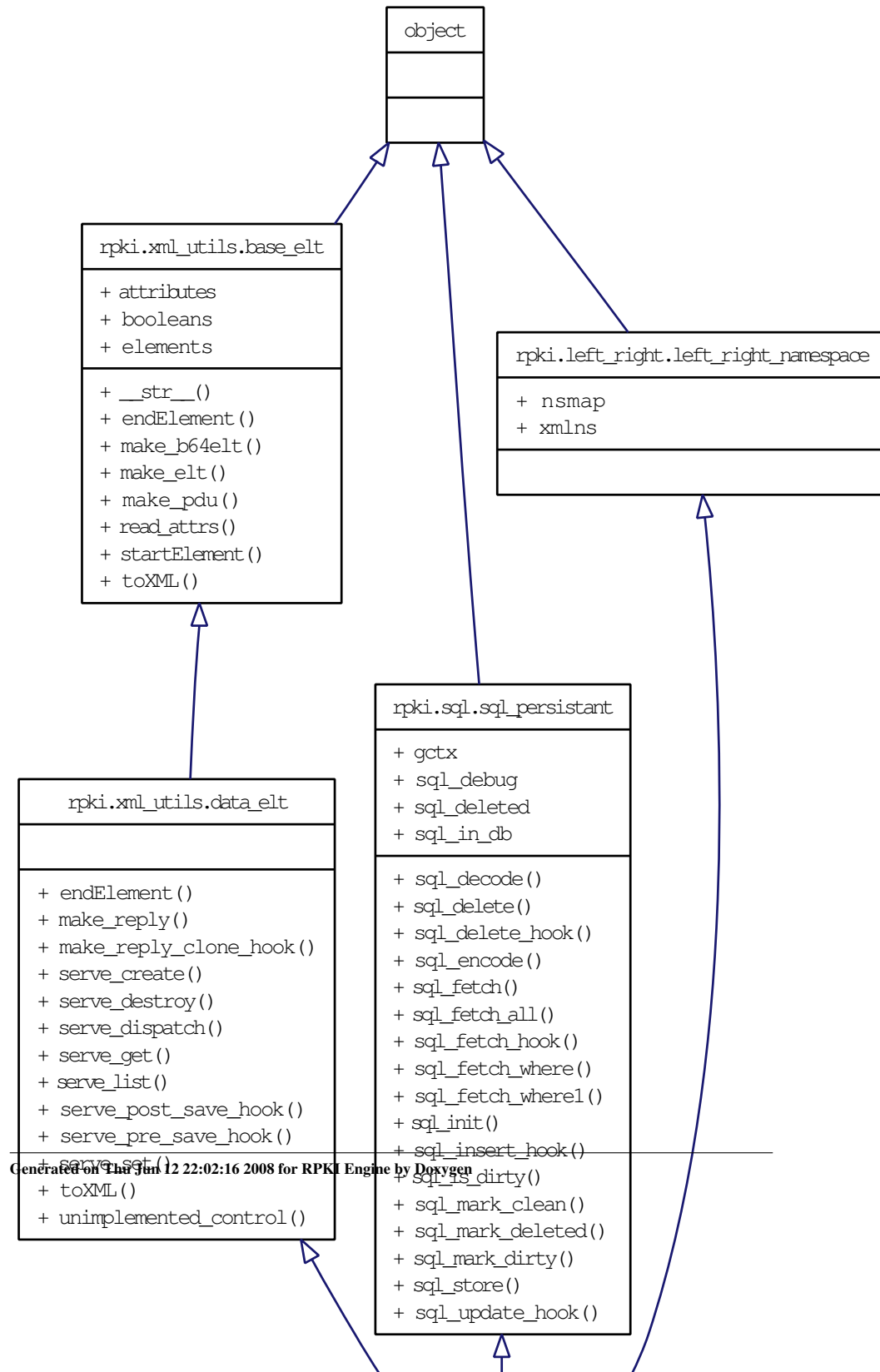
Definition at line 462 of file left_right.py.

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

- [left_right.py \(1873\)](#)

7.92 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](#)

7.92.1 Detailed Description

<route_origin/> element.

Definition at line 532 of file left_right.py.

7.92.2 Member Function Documentation

7.92.2.1 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.

7.92.2.2 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.

7.92.2.3 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.

7.92.2.4 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.

7.92.2.5 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.

7.92.2.6 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.

7.92.2.7 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.

7.92.2.8 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_persistent](#).

Definition at line 572 of file left_right.py.

7.92.2.9 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_persistent](#).

Definition at line 548 of file left_right.py.

7.92.2.10 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_persistent](#).

Definition at line 563 of file left_right.py.

7.92.2.11 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.

7.92.2.12 def rpki.left_right.route_origin_elt.update_roa (self)

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

Definition at line 597 of file left_right.py.

7.92.2.13 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.

7.92.3 Member Data Documentation**7.92.3.1 rpki.left_right.route_origin_elt.as_number**

Reimplemented in [irbe-cli.route_origin_elt](#).

Definition at line 591 of file left_right.py.

7.92.3.2 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.

7.92.3.3 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.

7.92.3.4 rpki.left_right.route_origin_elt.ca_detail_id = None [static]

Definition at line 544 of file left_right.py.

7.92.3.5 rpki.left_right.route_origin_elt.cert = None [static]

Definition at line 545 of file left_right.py.

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

Definition at line 535 of file left_right.py.

7.92.3.7 rpki.left_right.route_origin_elt.ipv4

Reimplemented in [irbe-cli.route_origin_elt](#).

Definition at line 550 of file left_right.py.

7.92.3.8 rpki.left_right.route_origin_elt.ipv6

Reimplemented in [irbe-cli.route_origin_elt](#).

Definition at line 556 of file left_right.py.

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

Definition at line 546 of file left_right.py.

7.92.3.10 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))
```

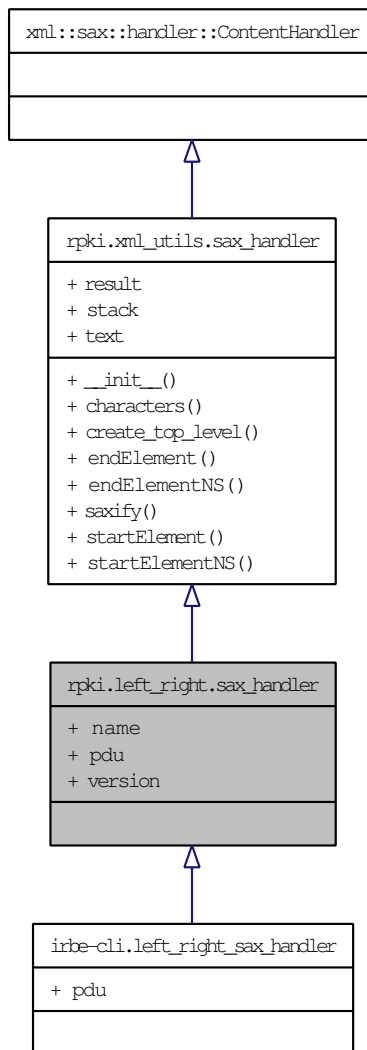
Definition at line 539 of file left_right.py.

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

- [left_right.py \(1873\)](#)

7.93 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"

7.93.1 Detailed Description

SAX handler for Left-Right protocol.

Definition at line 806 of file left_right.py.

7.93.2 Member Data Documentation

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

Definition at line 810 of file left_right.py.

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

Reimplemented in [irbe-cli.left_right_sax_handler](#).

Definition at line 809 of file left_right.py.

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

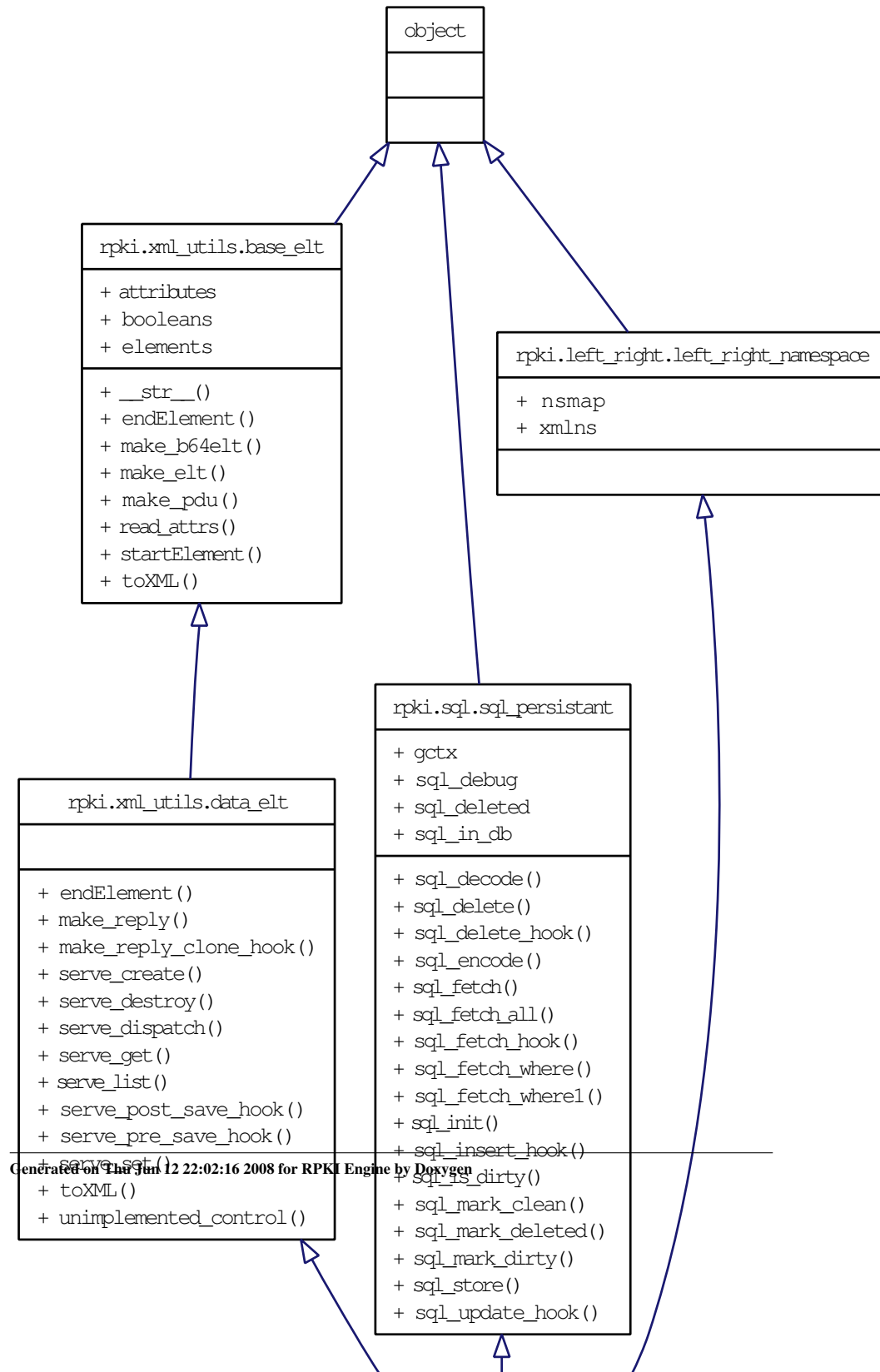
Definition at line 811 of file left_right.py.

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

- [left_right.py](#) (1873)

7.94 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

7.94.1 Detailed Description

<self/> element.

Definition at line 70 of file left_right.py.

7.94.2 Member Function Documentation

7.94.2.1 def rpki.left_right.self_elt.bsos (self)

Fetch all BSO objects that link to this self object.

Definition at line 88 of file left_right.py.

7.94.2.2 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.

7.94.2.3 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.

7.94.2.4 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.

7.94.2.5 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.

7.94.2.6 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.

7.94.2.7 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.

7.94.2.8 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.

7.94.2.9 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.

7.94.2.10 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.

7.94.2.11 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.

7.94.2.12 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.

7.94.2.13 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.

7.94.2.14 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.

7.94.3 Member Data Documentation

7.94.3.1 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.

7.94.3.2 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.

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

Definition at line 85 of file left_right.py.

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

Definition at line 86 of file left_right.py.

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

Definition at line 83 of file left_right.py.

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

Definition at line 73 of file left_right.py.

7.94.3.7 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.

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

Definition at line 84 of file left_right.py.

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

Definition at line 81 of file left_right.py.

7.94.3.10 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.

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

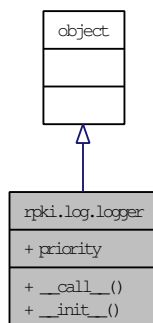
Definition at line 82 of file left_right.py.

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

- [left_right.py \(1873\)](#)

7.95 rpki.log.logger Class Reference

Inheritance diagram for rpki.log.logger:



Public Member Functions

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

Public Attributes

- [priority](#)

7.95.1 Detailed Description

Closure for logging.

Definition at line 38 of file log.py.

7.95.2 Member Function Documentation

7.95.2.1 `def rpki.log.logger.__call__(self, message)`

Definition at line 44 of file log.py.

7.95.2.2 `def rpki.log.logger.__init__(self, priority)`

Definition at line 41 of file log.py.

7.95.3 Member Data Documentation

7.95.3.1 rpki.log.logger.priority

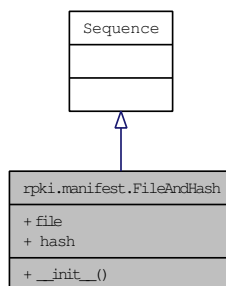
Definition at line 42 of file log.py.

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

- [log.py \(1873\)](#)

7.96 rpki.manifest.FileAndHash Class Reference

Inheritance diagram for rpki.manifest.FileAndHash:



Public Member Functions

- [def `__init__`](#)

Public Attributes

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

7.96.1 Detailed Description

Definition at line 26 of file manifest.py.

7.96.2 Member Function Documentation

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

Definition at line 27 of file manifest.py.

7.96.3 Member Data Documentation

7.96.3.1 rpki.manifest.FileAndHash.file

Definition at line 28 of file manifest.py.

7.96.3.2 rpki.manifest.FileAndHash.hash

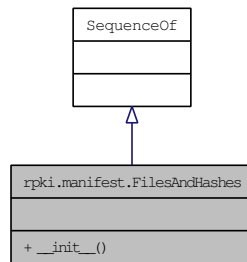
Definition at line 29 of file manifest.py.

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

- [manifest.py \(1873\)](#)

7.97 rpki.manifest.FilesAndHashes Class Reference

Inheritance diagram for rpki.manifest.FilesAndHashes:



Public Member Functions

- [def __init__](#)

7.97.1 Detailed Description

Definition at line 33 of file manifest.py.

7.97.2 Member Function Documentation

7.97.2.1 def rpki.manifest.FilesAndHashes.__init__ (self, optional = 0, default = ")

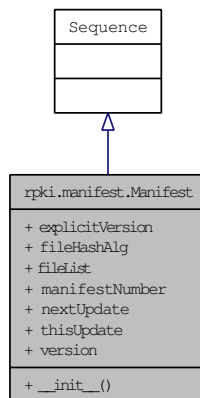
Definition at line 34 of file manifest.py.

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

- [manifest.py \(1873\)](#)

7.98 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`

7.98.1 Detailed Description

Definition at line 37 of file `manifest.py`.

7.98.2 Member Function Documentation

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

Definition at line 38 of file manifest.py.

7.98.3 Member Data Documentation

7.98.3.1 rpki.manifest.Manifest.explicitVersion

Definition at line 40 of file manifest.py.

7.98.3.2 rpki.manifest.Manifest.fileHashAlg

Definition at line 44 of file manifest.py.

7.98.3.3 rpki.manifest.Manifest.fileList

Definition at line 45 of file manifest.py.

7.98.3.4 rpki.manifest.Manifest.manifestNumber

Definition at line 41 of file manifest.py.

7.98.3.5 rpki.manifest.Manifest.nextUpdate

Definition at line 43 of file manifest.py.

7.98.3.6 rpki.manifest.Manifest.thisUpdate

Definition at line 42 of file manifest.py.

7.98.3.7 rpki.manifest.Manifest.version

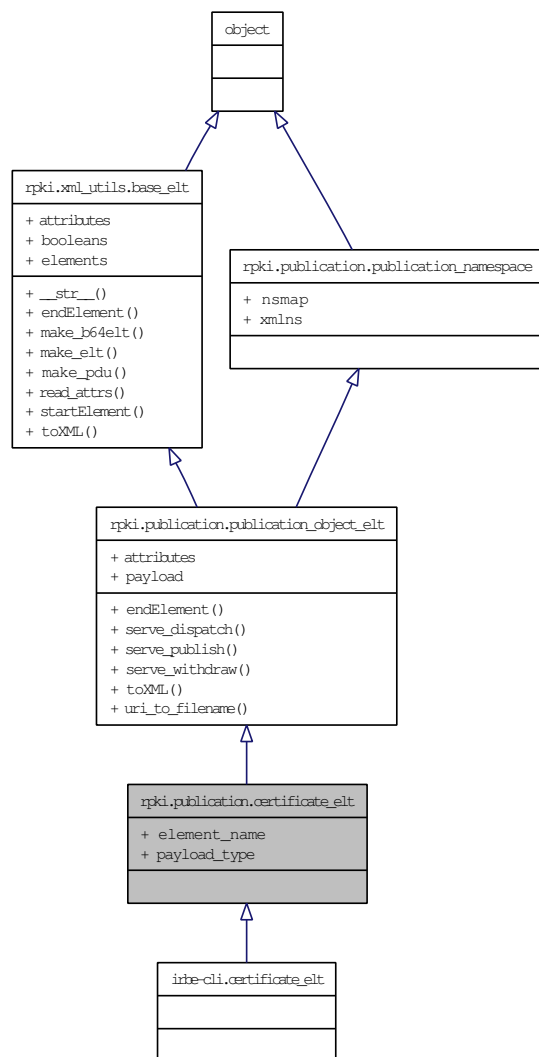
Definition at line 39 of file manifest.py.

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

- [manifest.py \(1873\)](#)

7.99 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`

7.99.1 Detailed Description

`<certificate/> element.`

Definition at line 205 of file `publication.py`.

7.99.2 Member Data Documentation

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

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

7.99.2.2 `rpki.publication.certificate_elt.payload_type = rpki.x509.X509`
[static]

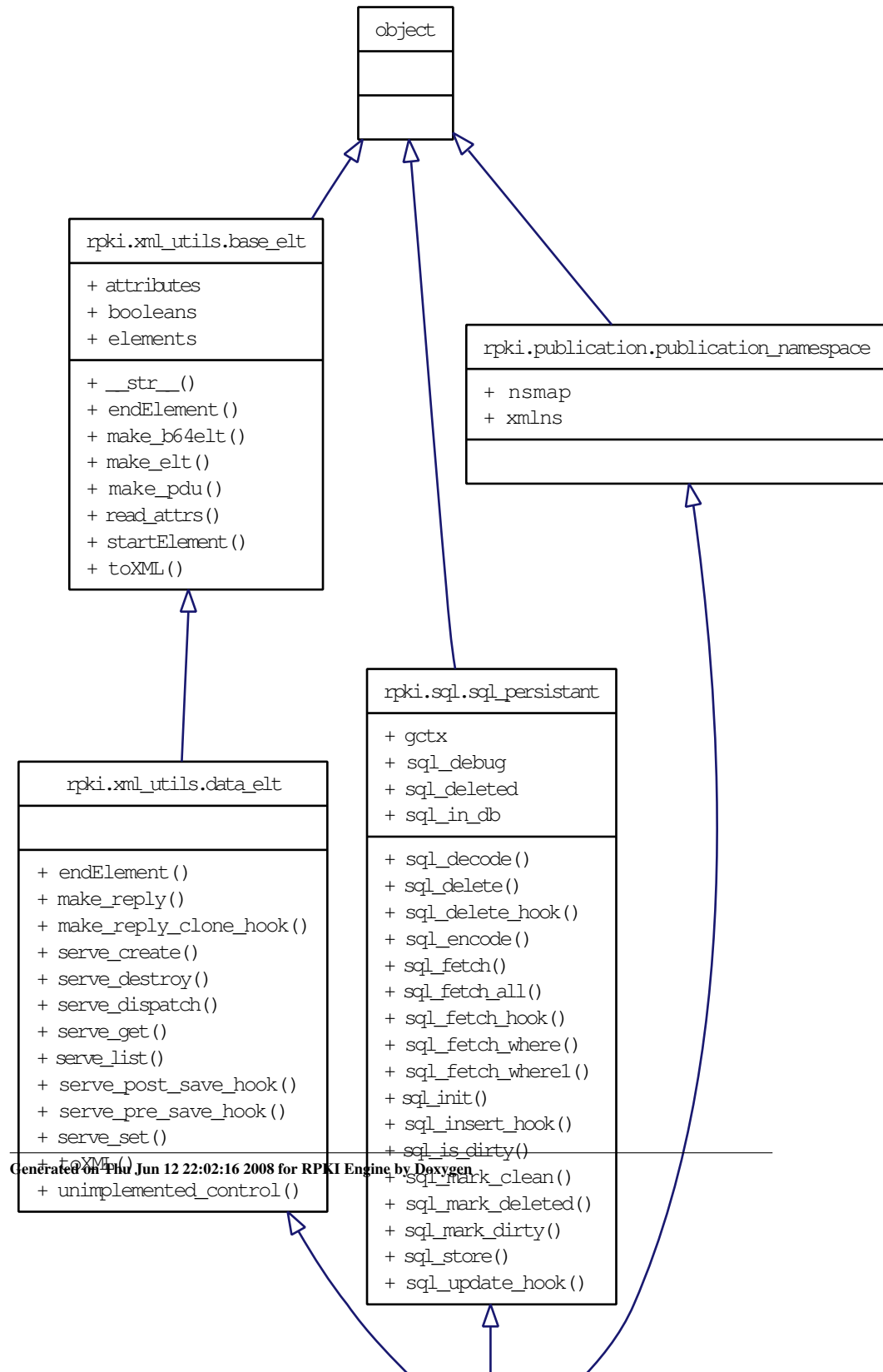
Definition at line 209 of file `publication.py`.

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

- [publication.py \(1873\)](#)

7.100 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](#)))

7.100.1 Detailed Description

<client/> element.

Definition at line 91 of file publication.py.

7.100.2 Member Function Documentation

7.100.2.1 def rpki.publication.client_elt.check_allowed_uri (self, uri)

Definition at line 134 of file publication.py.

7.100.2.2 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.

7.100.2.3 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.

7.100.2.4 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.

7.100.2.5 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.

7.100.3 Member Data Documentation

7.100.3.1 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.

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

Definition at line 100 of file publication.py.

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

Definition at line 101 of file publication.py.

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

Definition at line 102 of file publication.py.

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

Definition at line 104 of file publication.py.

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

Definition at line 94 of file publication.py.

7.100.3.7 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.

7.100.3.8 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]

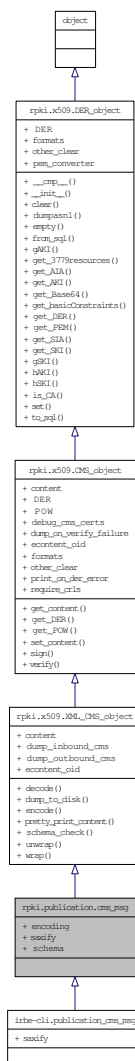
Definition at line 98 of file publication.py.

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

- [publication.py \(1873\)](#)

7.101 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`

7.101.1 Detailed Description

Class to hold a CMS-signed publication PDU.

Definition at line 277 of file publication.py.

7.101.2 Member Data Documentation

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

Definition at line 280 of file publication.py.

7.101.2.2 `rpki.publication.cms_msg.saxify = sax_handler.saxify [static]`

Reimplemented in [irbe-cli.publication_cms_msg](#).

Definition at line 282 of file publication.py.

7.101.2.3 `rpki.publication.cms_msg.schema = rpki.relaxng.publication [static]`

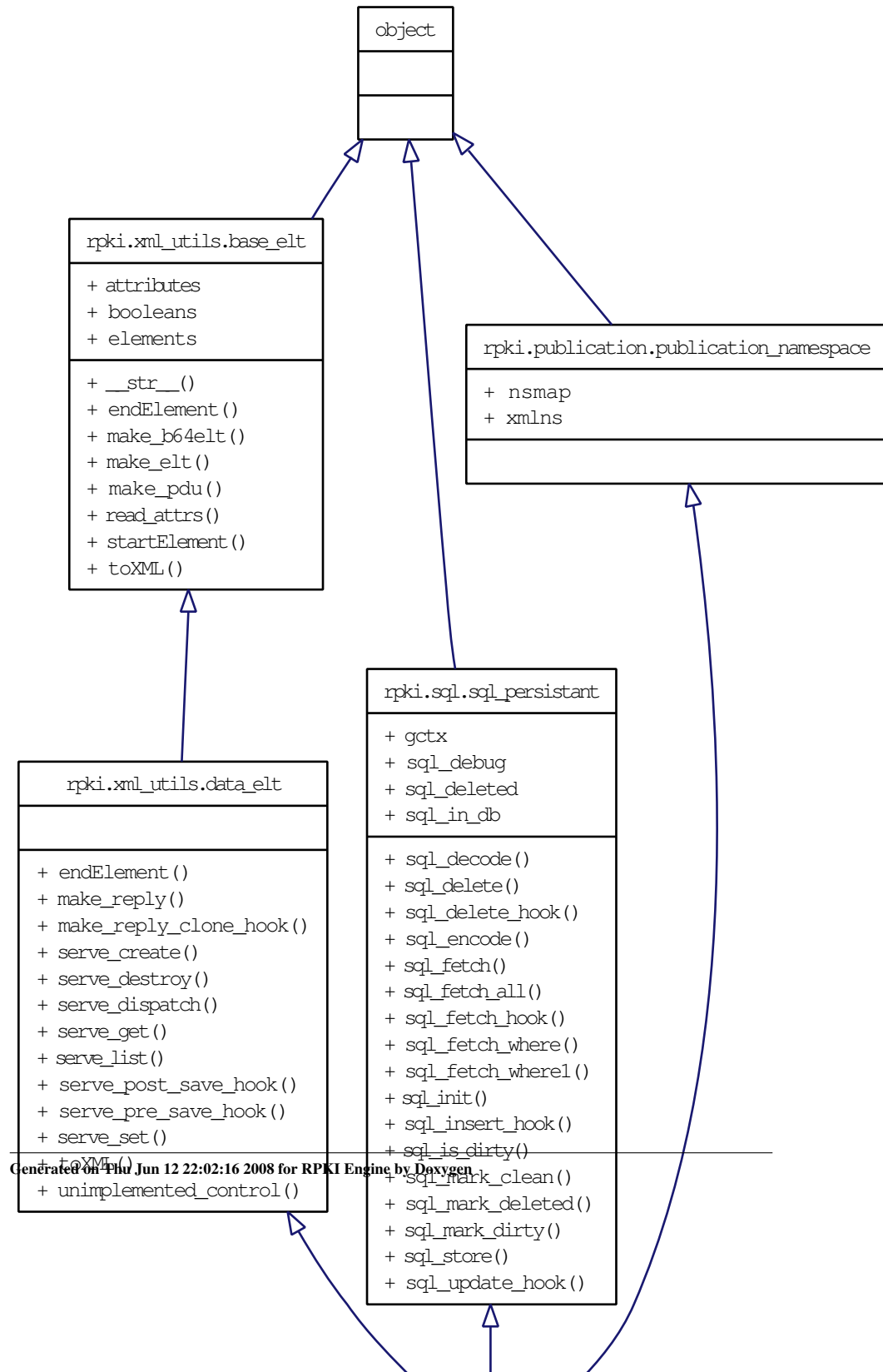
Definition at line 281 of file publication.py.

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

- [publication.py \(1873\)](#)

7.102 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

7.102.1 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`.

7.102.2 Member Function Documentation

7.102.2.1 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`.

7.102.2.2 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.

7.102.2.3 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.

7.102.2.4 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.

7.102.3 Member Data Documentation**7.102.3.1 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.

7.102.3.2 rpki.publication.config_elt.config_id

Definition at line 64 of file publication.py.

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

Definition at line 52 of file publication.py.

7.102.3.4 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`.

7.102.3.5 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`.

7.102.3.6 int `rpki.publication.config_elt.wired_in_config_id` = 1 [static]

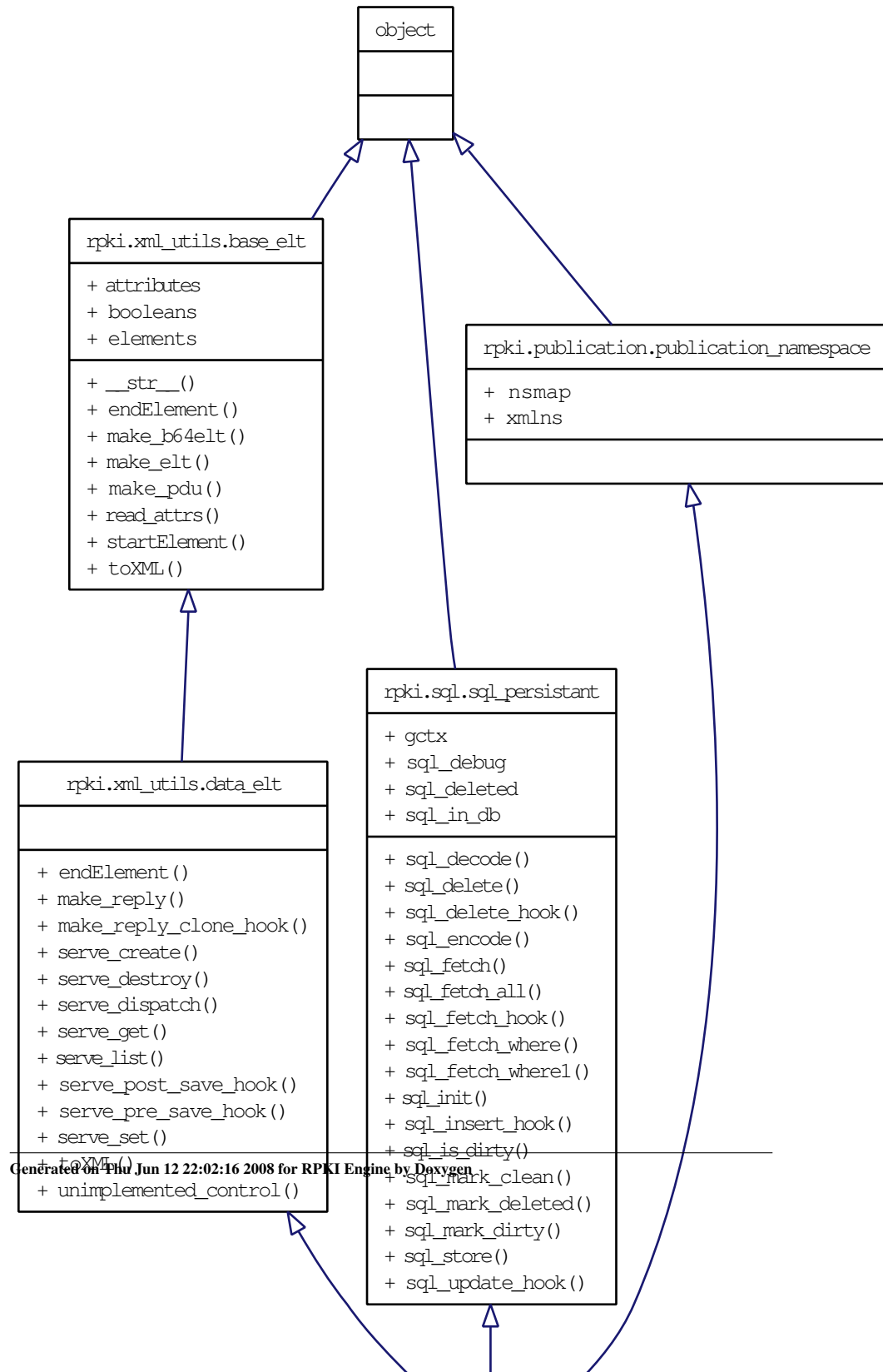
Definition at line 57 of file `publication.py`.

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

- [publication.py](#) (1873)

7.103 rpki.publication.control_elt Class Reference

Inheritance diagram for rpki.publication.control_elt:



Public Member Functions

- [def serve_dispatch](#)

7.103.1 Detailed Description

Virtual class for control channel objects.

Definition at line 30 of file publication.py.

7.103.2 Member Function Documentation

7.103.2.1 `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.

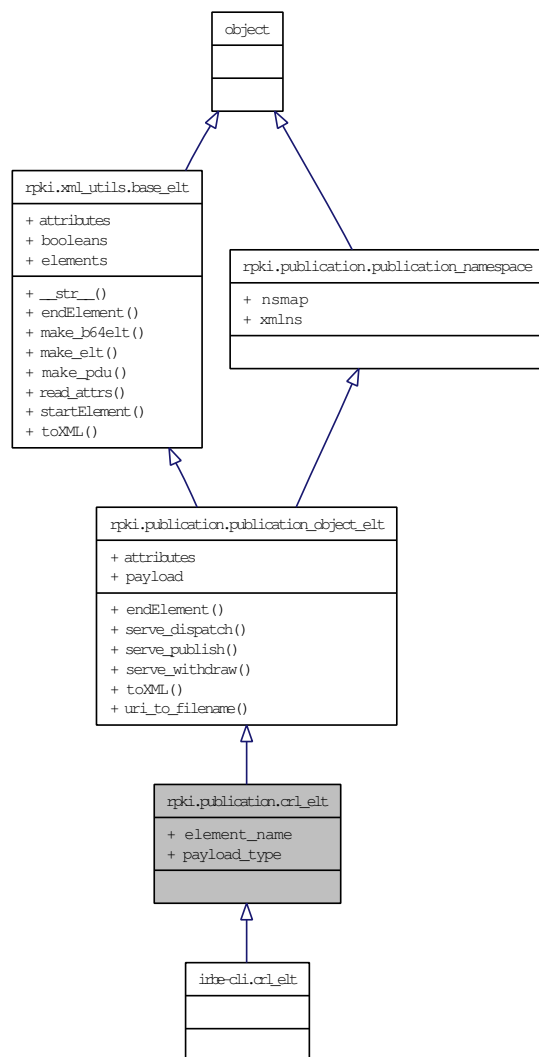
Definition at line 33 of file publication.py.

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

- [publication.py \(1873\)](#)

7.104 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`

7.104.1 Detailed Description

`<crl/> element.`

Definition at line 211 of file publication.py.

7.104.2 Member Data Documentation

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

Definition at line 214 of file publication.py.

7.104.2.2 `rpki.publication.crl_elt.payload_type = rpki.x509.CRL [static]`

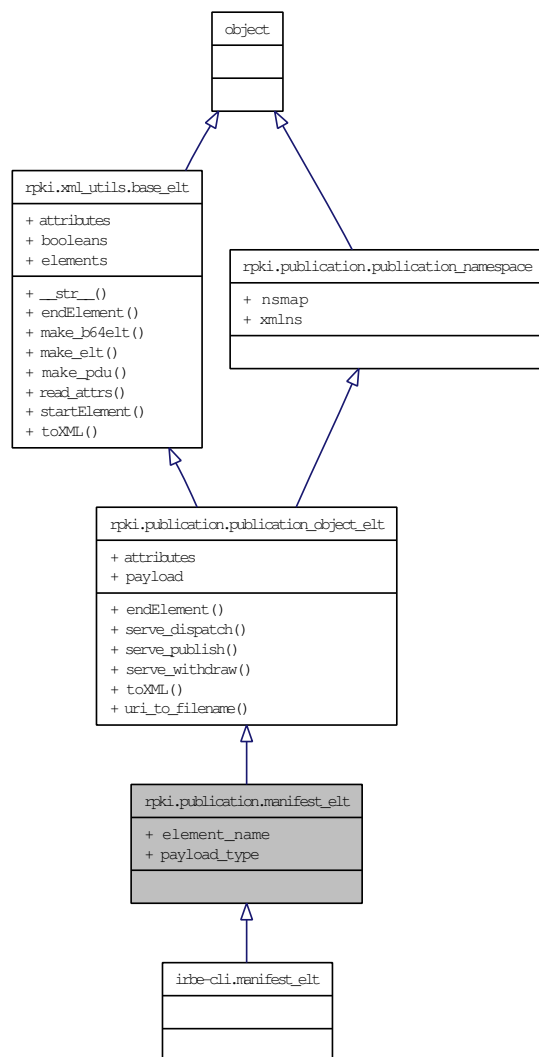
Definition at line 215 of file publication.py.

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

- [publication.py \(1873\)](#)

7.105 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`

7.105.1 Detailed Description

`<manifest/> element.`

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

7.105.2 Member Data Documentation

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

Definition at line 220 of file `publication.py`.

7.105.2.2 `rpki.publication.manifest_elt.payload_type` =
`rpki.x509.SignedManifest` [static]

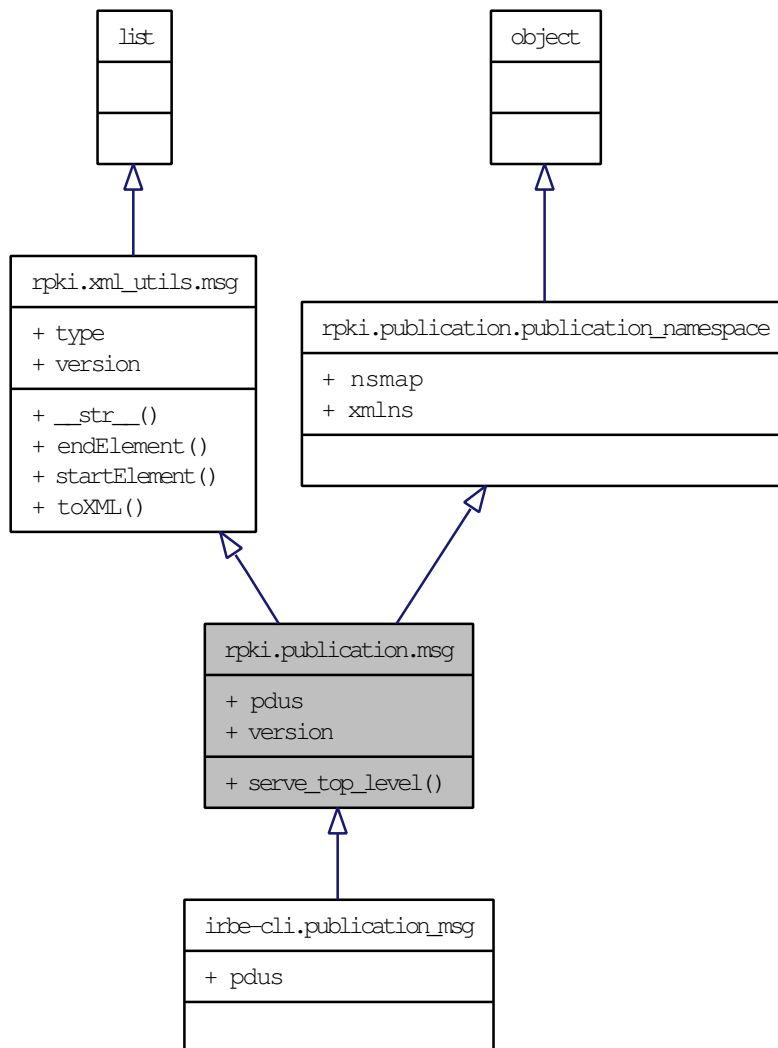
Definition at line 221 of file `publication.py`.

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

- [publication.py \(1873\)](#)

7.106 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.

7.106.1 Detailed Description

Publication PDU.

Definition at line 247 of file publication.py.

7.106.2 Member Function Documentation

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

Serve one msg PDU.

Definition at line 259 of file publication.py.

7.106.3 Member Data Documentation

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

Initial value:

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

Dispatch table of PDUs for this protocol.

Reimplemented in [irbe-cli.publication_msg](#).

Definition at line 256 of file publication.py.

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

Protocol version.

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

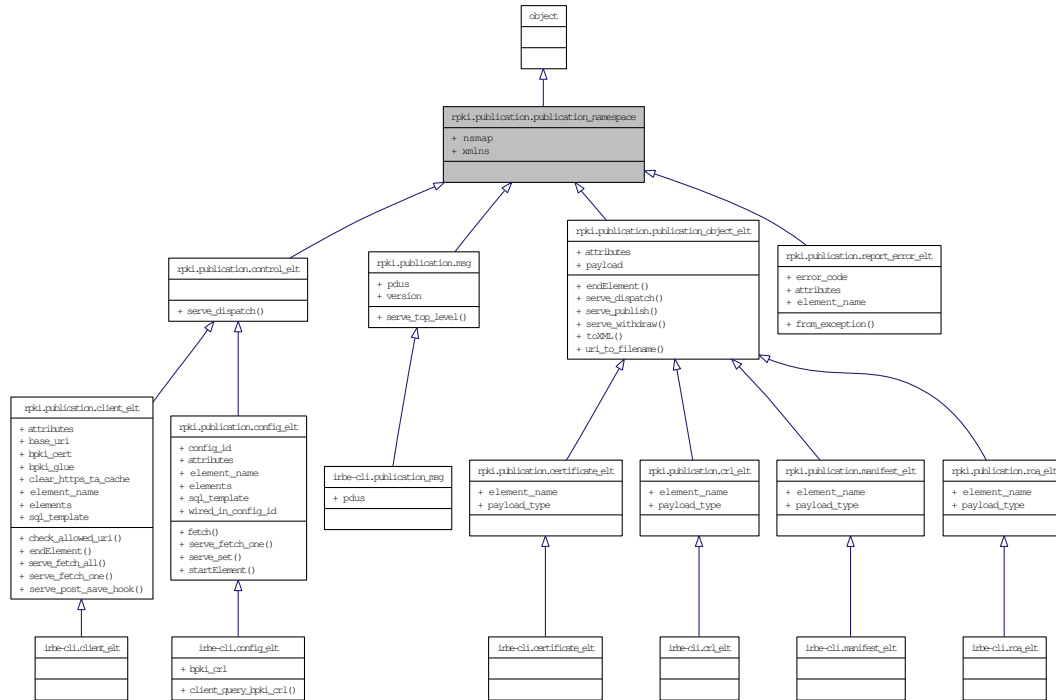
Definition at line 252 of file publication.py.

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

- [publication.py \(1873\)](#)

7.107 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/"

7.107.1 Detailed Description

XML namespace parameters for publication protocol.

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

7.107.2 Member Data Documentation

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

Definition at line 28 of file `publication.py`.

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

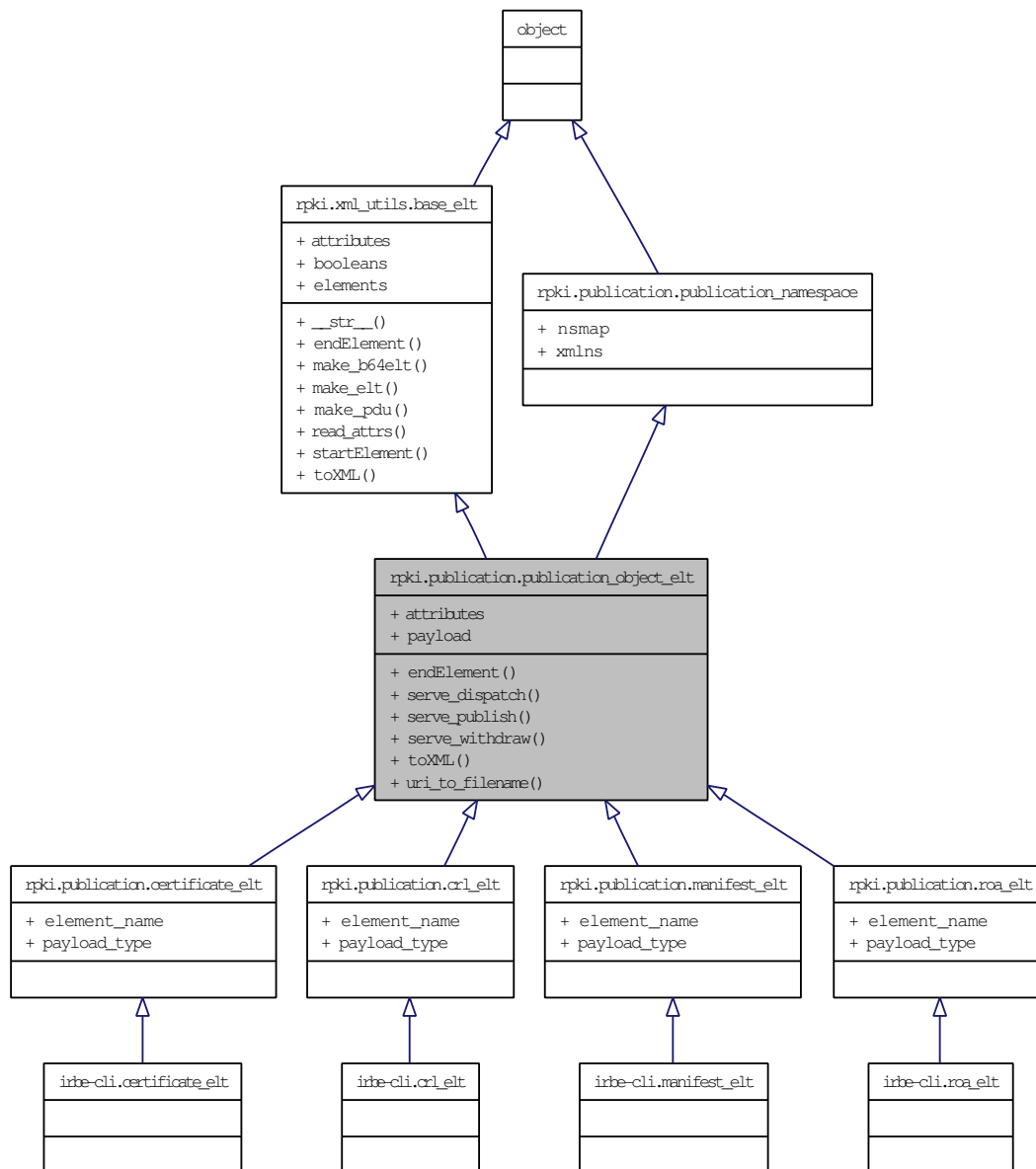
Definition at line 27 of file `publication.py`.

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

- [publication.py \(1873\)](#)

7.108 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

7.108.1 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.

7.108.2 Member Function Documentation

7.108.2.1 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.

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

Action dispatch handler.

Definition at line 164 of file publication.py.

7.108.2.3 def rpki.publication.publication_object_elt.serve_publish (self)

Publish an object.

Definition at line 180 of file publication.py.

7.108.2.4 def rpki.publication.publication_object_elt.serve_withdraw (self)

Withdraw an object.

Definition at line 191 of file publication.py.

7.108.2.5 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.

7.108.2.6 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.

7.108.3 Member Data Documentation**7.108.3.1 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.

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

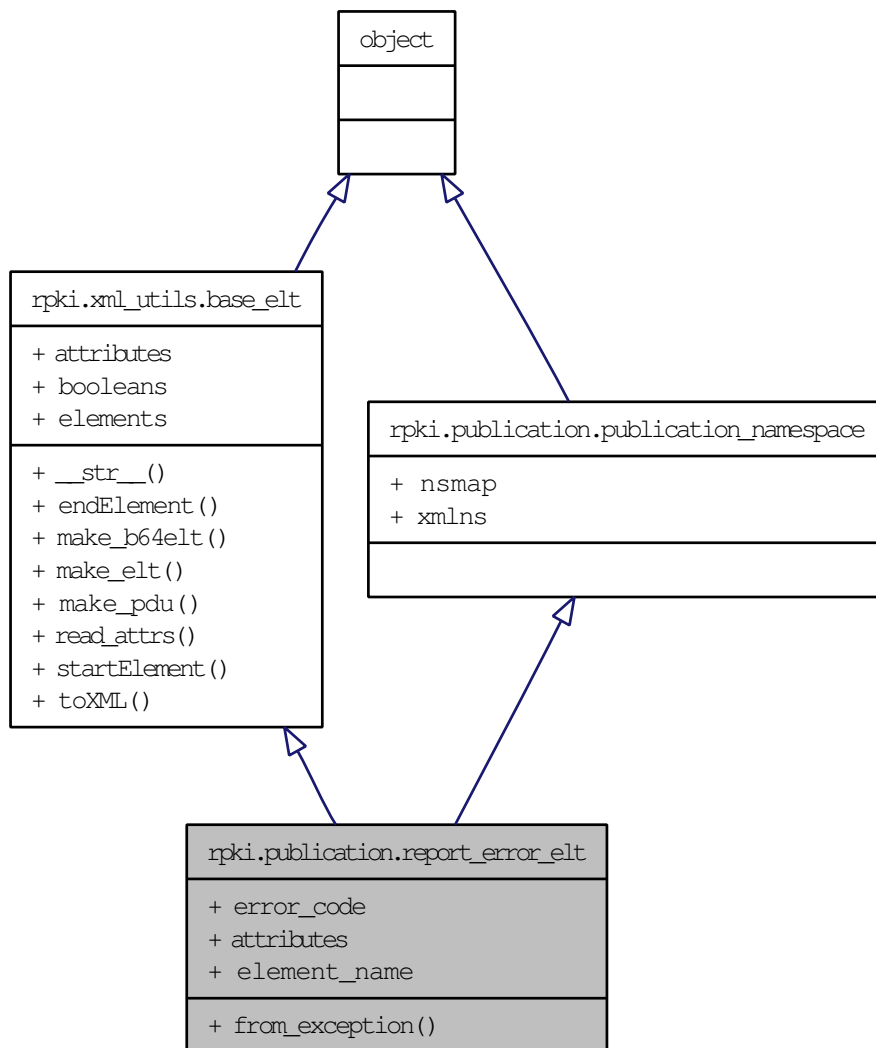
Definition at line 148 of file publication.py.

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

- [publication.py \(1873\)](#)

7.109 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"

7.109.1 Detailed Description

<report_error/> element.

Definition at line 234 of file publication.py.

7.109.2 Member Function Documentation

7.109.2.1 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.

7.109.3 Member Data Documentation

7.109.3.1 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.

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

Definition at line 237 of file publication.py.

7.109.3.3 rpki.publication.report_error_elt.error_code

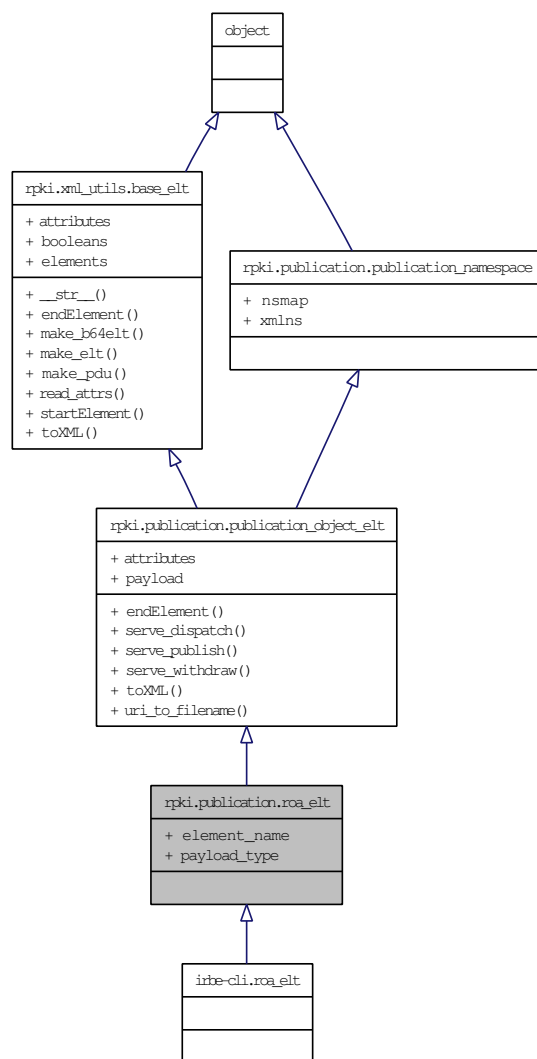
Definition at line 244 of file publication.py.

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

- [publication.py \(1873\)](#)

7.110 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](#)

7.110.1 Detailed Description

<roa/> element.

Definition at line 223 of file publication.py.

7.110.2 Member Data Documentation

7.110.2.1 string [rpki.publication.roa_elt.element_name](#) = "roa" [static]

Definition at line 226 of file publication.py.

7.110.2.2 [rpki.publication.roa_elt.payload_type](#) = [rpki.x509.ROA](#) [static]

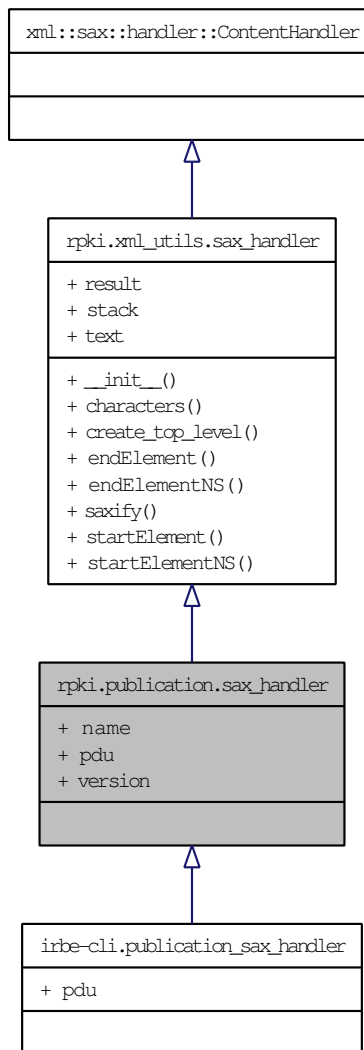
Definition at line 227 of file publication.py.

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

- [publication.py](#) (1873)

7.111 rpki.publication.sax_handler Class Reference

Inheritance diagram for rpki.publication.sax_handler:



Static Public Attributes

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

7.111.1 Detailed Description

SAX handler for publication protocol.

Definition at line 270 of file publication.py.

7.111.2 Member Data Documentation

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

Definition at line 274 of file publication.py.

7.111.2.2 `rpki.publication.sax_handler.pdu = msg [static]`

Reimplemented in [irbe-cli.publication_sax_handler](#).

Definition at line 273 of file publication.py.

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

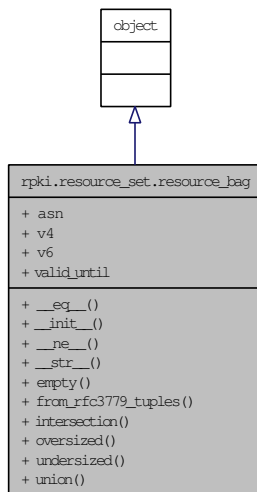
Definition at line 275 of file publication.py.

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

- [publication.py \(1873\)](#)

7.112 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.

7.112.1 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.

7.112.2 Member Function Documentation

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

Definition at line 508 of file resource_set.py.

7.112.2.2 `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.

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

Definition at line 514 of file resource_set.py.

7.112.2.4 `def rpki.resource_set.resource_bag.__str__(self)`

Definition at line 535 of file resource_set.py.

7.112.2.5 `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.

7.112.2.6 `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.

7.112.2.7 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.

7.112.2.8 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.

7.112.2.9 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.

7.112.2.10 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.

7.112.3 Member Data Documentation**7.112.3.1 rpki::resource_set.resource_bag::asn**

Set of Autonomous System Number resources.

Definition at line 466 of file resource_set.py.

7.112.3.2 rpki::resource_set.resource_bag::v4

Set of IPv4 resources.

Definition at line 467 of file resource_set.py.

7.112.3.3 rpki::resource_set.resource_bag::v6

Set of IPv6 resources.

Definition at line 468 of file resource_set.py.

7.112.3.4 rpki::resource_set.resource_bag::valid_until

Expiration date of resources, for setting certificate notAfter field.

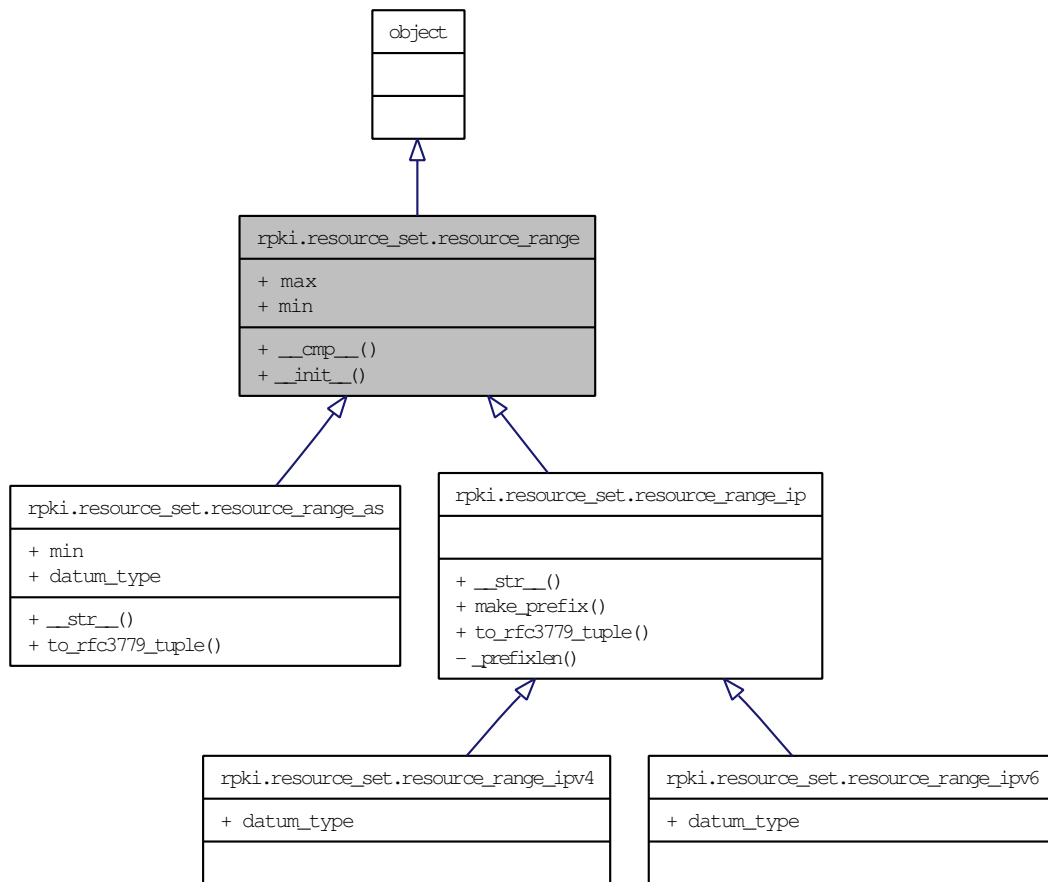
Definition at line 469 of file resource_set.py.

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

- [resource_set.py \(1873\)](#)

7.113 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](#)

7.113.1 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.

7.113.2 Member Function Documentation

7.113.2.1 `def rpki.resource_set.resource_range.__cmp__(self, other)`

Compare two resource_range objects.

Definition at line 49 of file resource_set.py.

7.113.2.2 `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.

7.113.3 Member Data Documentation

7.113.3.1 `rpki.resource_set.resource_range.max`

Definition at line 47 of file resource_set.py.

7.113.3.2 rpki.resource_set.resource_range.min

Reimplemented in [rpki.resource_set.resource_range_as](#).

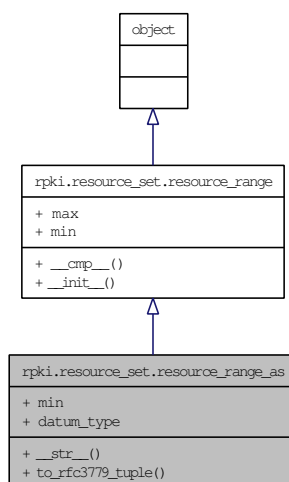
Definition at line 46 of file resource_set.py.

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

- [resource_set.py](#) (1873)

7.114 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).

7.114.1 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`.

7.114.2 Member Function Documentation

7.114.2.1 `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`.

7.114.2.2 `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`.

7.114.3 Member Data Documentation

7.114.3.1 `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`.

7.114.3.2 `rpki.resource_set.resource_range_as.min`

Reimplemented from [rpki.resource_set.resource_range](#).

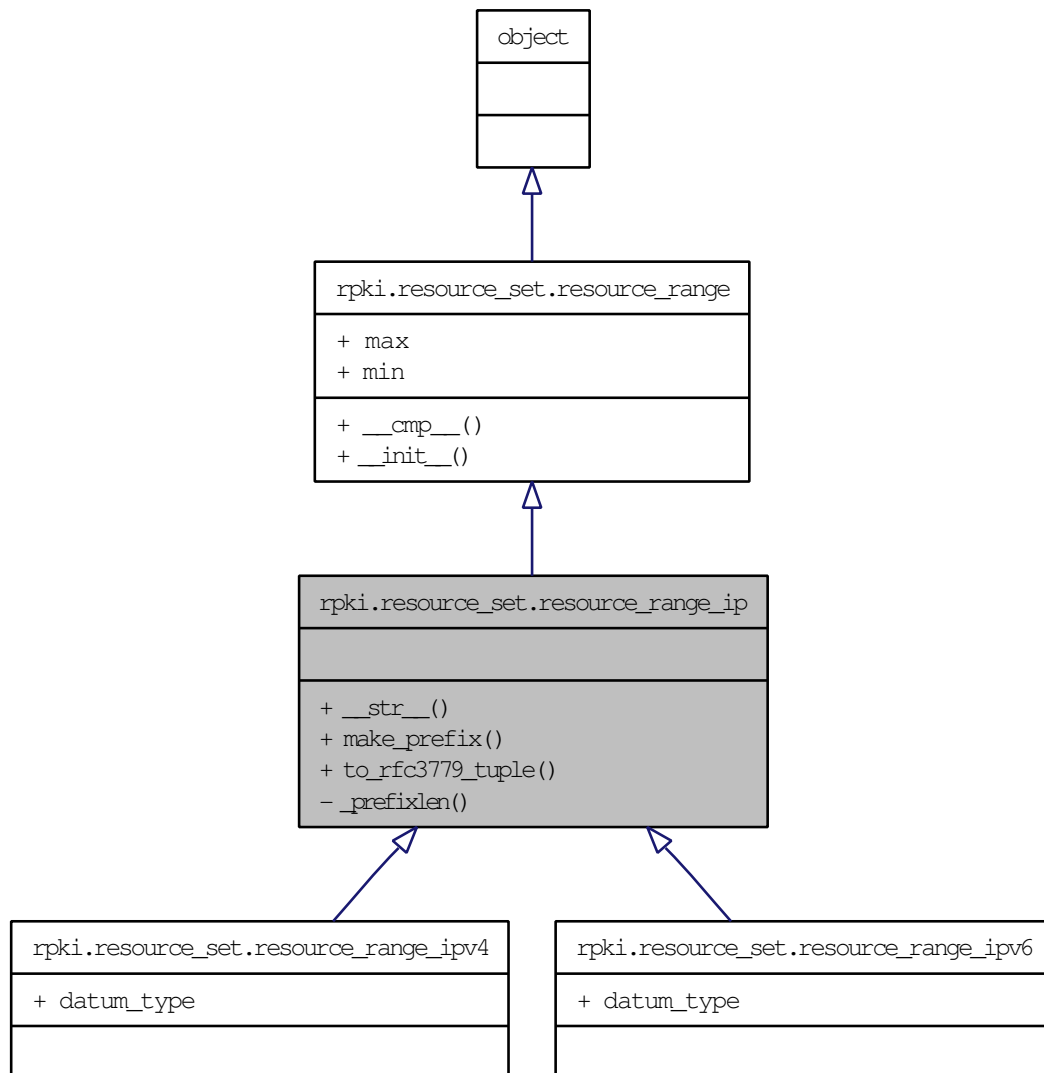
Definition at line 71 of file `resource_set.py`.

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

- [resource_set.py \(1873\)](#)

7.115 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](#)

7.115.1 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.

7.115.2 Member Function Documentation

7.115.2.1 `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.

7.115.2.2 `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.

7.115.2.3 `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.

7.115.2.4 `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.

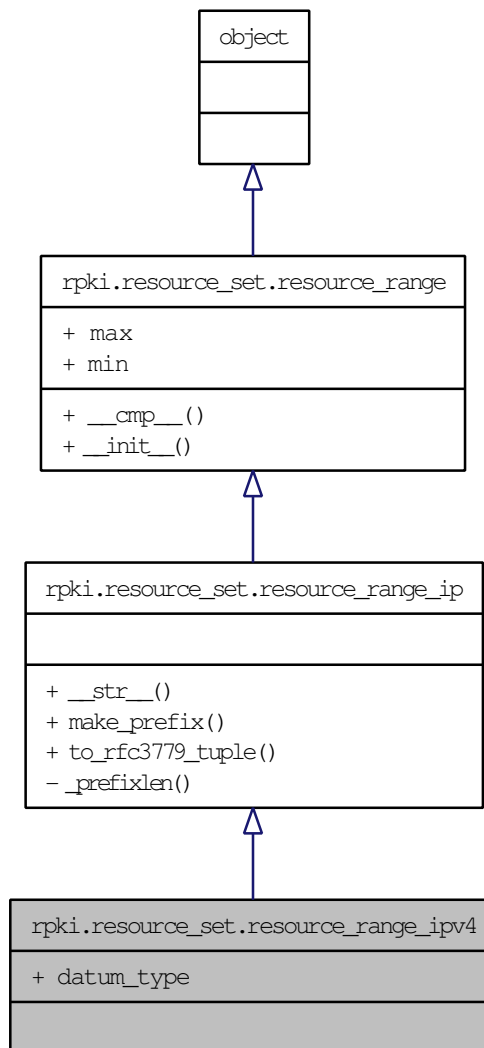
Definition at line 114 of file resource_set.py.

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

- [resource_set.py \(1873\)](#)

7.116 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).

7.116.1 Detailed Description

Range of IPv4 addresses.

Definition at line 132 of file `resource_set.py`.

7.116.2 Member Data Documentation

7.116.2.1 `rpki::resource_set.resource_range_ipv4::datum_type` =
`rpki.ipaddr.v4addr` `[static]`

Type of underlying data (min and max).

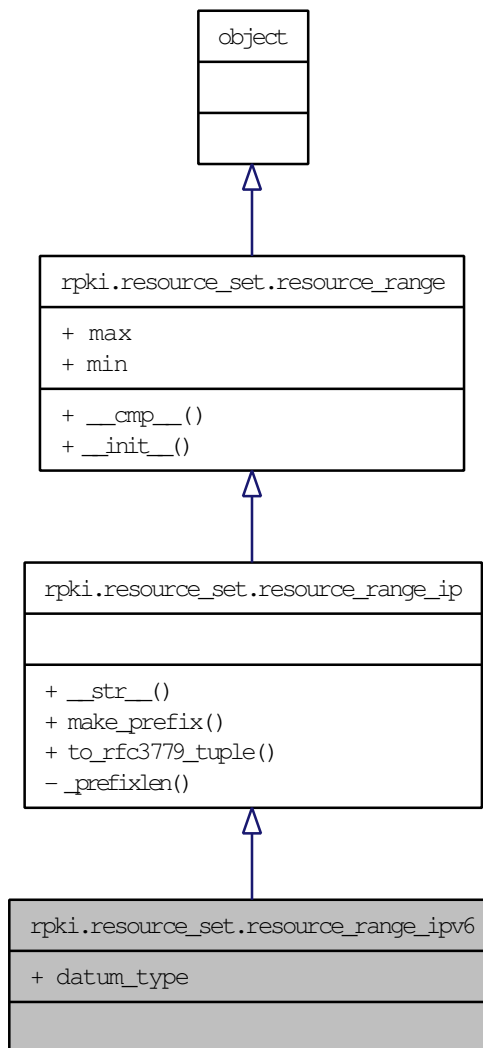
Definition at line 138 of file `resource_set.py`.

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

- [resource_set.py \(1873\)](#)

7.117 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).

7.117.1 Detailed Description

Range of IPv6 addresses.

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

7.117.2 Member Data Documentation

7.117.2.1 `rpki::resource_set.resource_range_ipv6::datum_type` =
`rpki.ipaddr.v6addr` [`static`]

Type of underlying data (min and max).

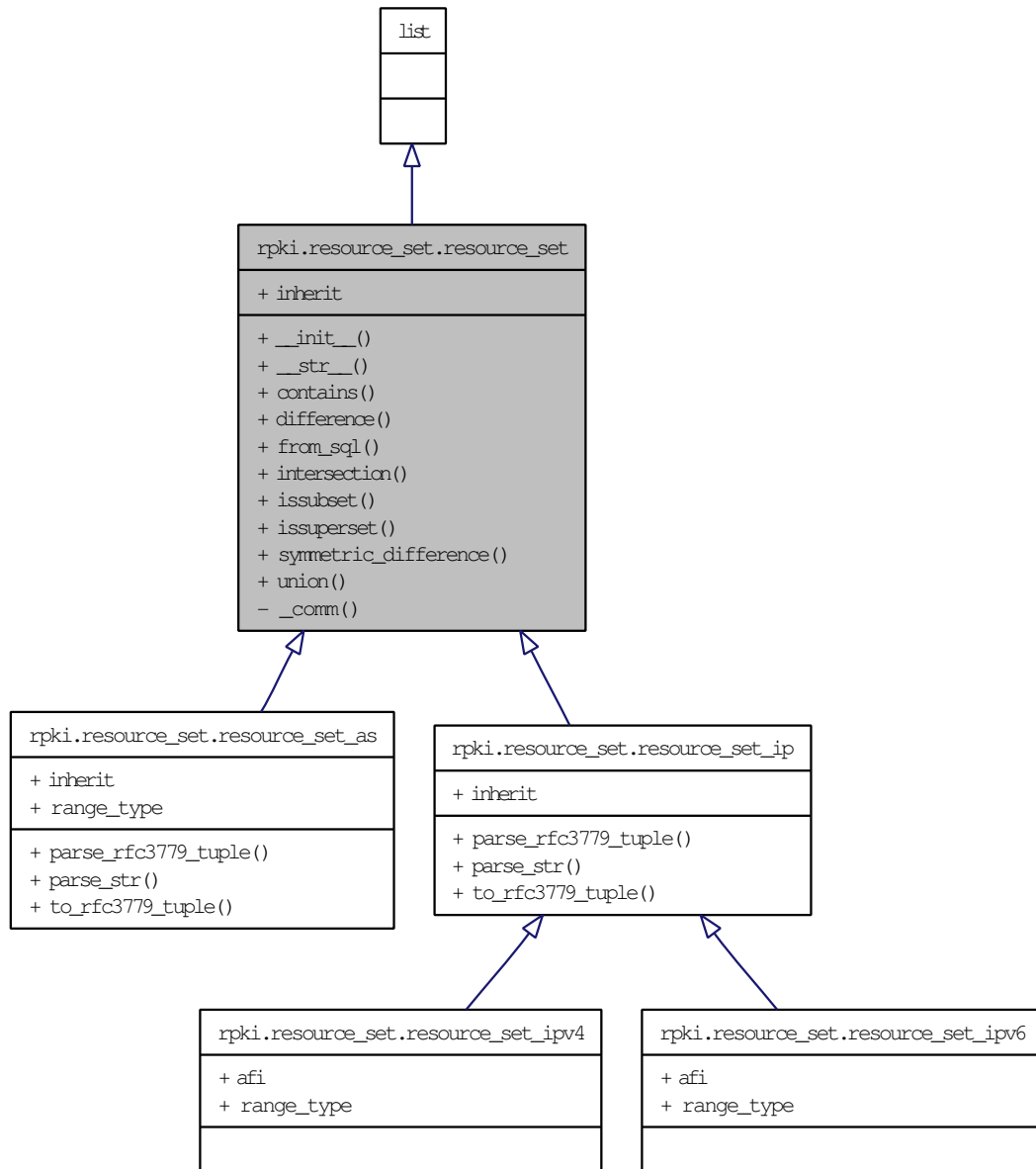
Definition at line 146 of file `resource_set.py`.

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

- [resource_set.py \(1873\)](#)

7.118 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`

7.118.1 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`.

7.118.2 Member Function Documentation

7.118.2.1 `def rpki.resource_set.resource_set.__init__(self, ini = None)`

Initialize a `resource_set`.

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

7.118.2.2 def rpki.resource_set.resource_set.__str__ (self)

Convert a resource_set to string format.

Definition at line 199 of file resource_set.py.

7.118.2.3 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.

7.118.2.4 def rpki.resource_set.resource_set.contains (self, item)

Set membership test for resource sets.

Definition at line 274 of file resource_set.py.

7.118.2.5 def rpki.resource_set.resource_set.difference (self, other)

Set difference for resource sets.

Definition at line 265 of file resource_set.py.

7.118.2.6 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.

7.118.2.7 def rpki.resource_set.resource_set.intersection (self, other)

Set intersection for resource sets.

Definition at line 261 of file resource_set.py.

7.118.2.8 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.

7.118.2.9 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.

7.118.2.10 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.

7.118.2.11 def rpki.resource_set.resource_set.union (self, other)

Set union for resource sets.

Definition at line 238 of file resource_set.py.

7.118.3 Member Data Documentation**7.118.3.1 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](#).

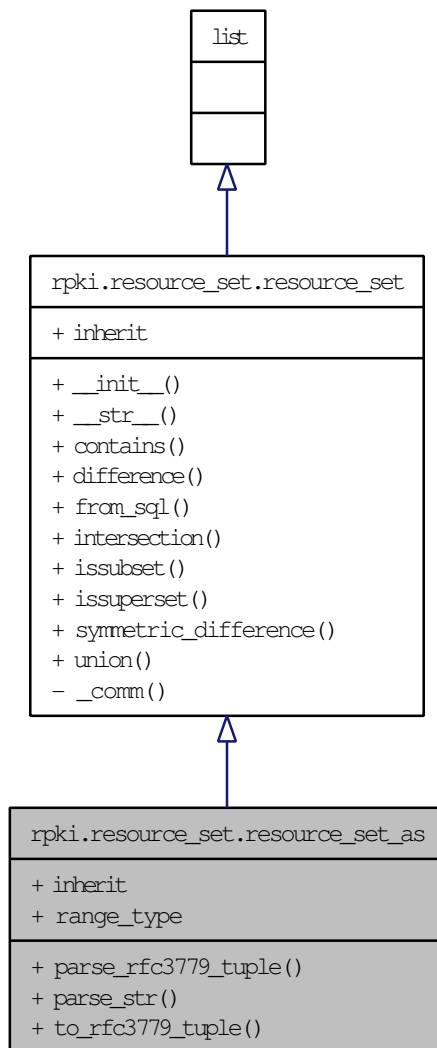
Definition at line 173 of file resource_set.py.

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

- [resource_set.py](#) (1873)

7.119 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](#).

7.119.1 Detailed Description

ASN resource set.

Definition at line 312 of file resource_set.py.

7.119.2 Member Function Documentation

7.119.2.1 `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.

7.119.2.2 `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.

7.119.2.3 `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.

7.119.3 Member Data Documentation

7.119.3.1 `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`.

7.119.3.2 `rpki::resource_set.resource_set_as::range_type = resource_range_as` [static]

Type of range underlying this type of [resource_set](#).

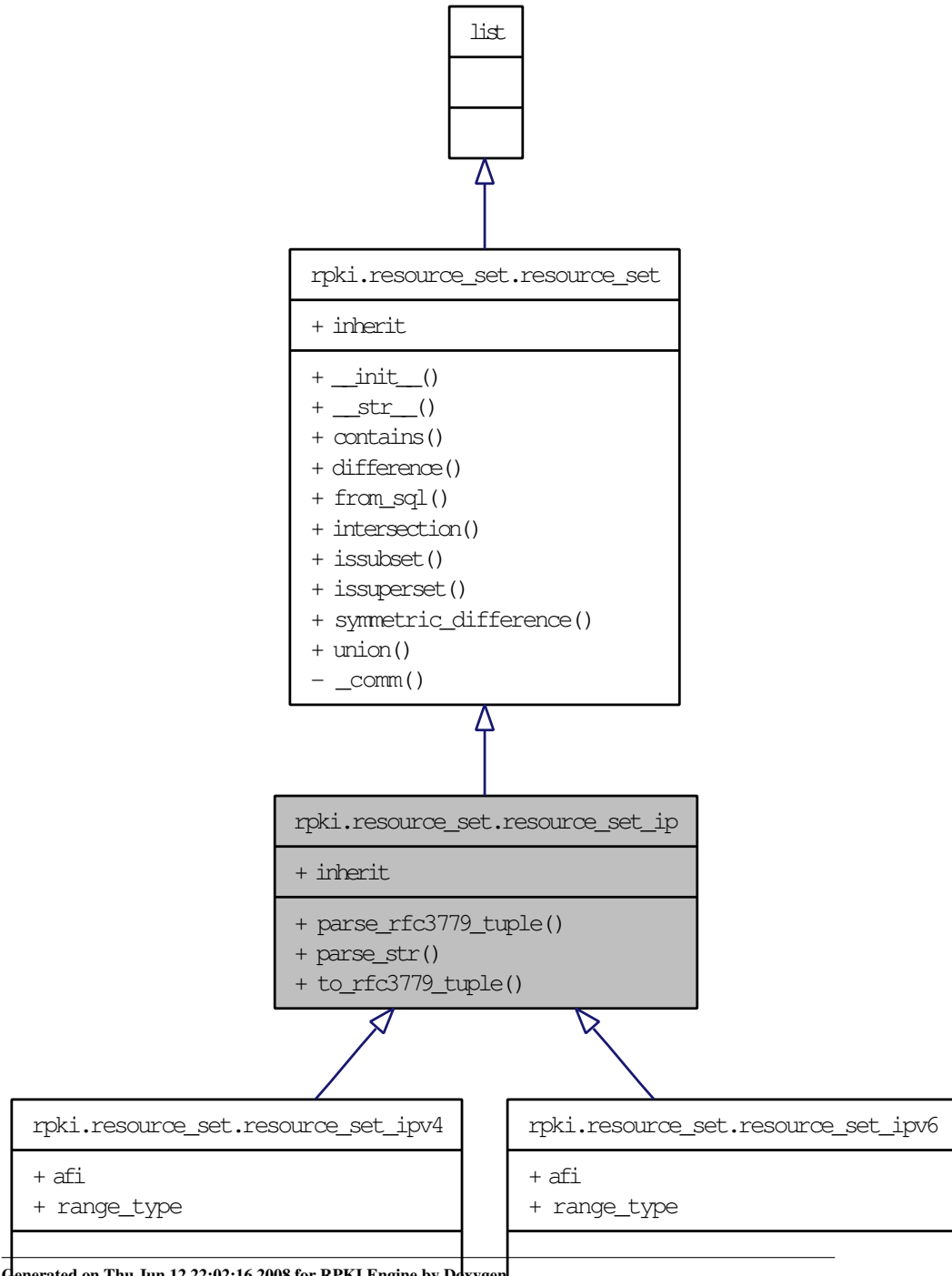
Definition at line 318 of file `resource_set.py`.

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

- [resource_set.py](#) (1873)

7.120 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.

7.120.1 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.

7.120.2 Member Function Documentation

7.120.2.1 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.

7.120.2.2 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.

7.120.2.3 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.

7.120.3 Member Data Documentation

7.120.3.1 rpki.resource_set.resource_set_ip.inherit

Boolean indicating whether this [resource_set](#) uses RFC 3779 inheritance.

Reimplemented from [rpki.resource_set.resource_set](#).

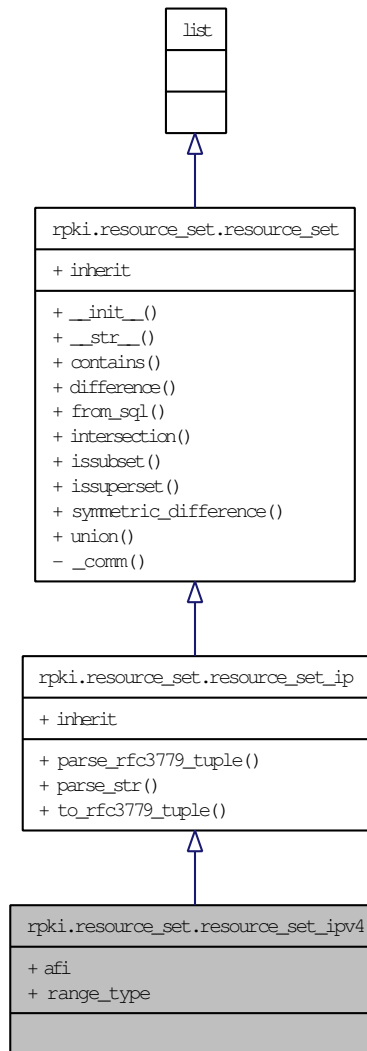
Definition at line 385 of file resource_set.py.

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

- [resource_set.py](#) (1873)

7.121 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](#).

7.121.1 Detailed Description

IPv4 address resource set.

Definition at line 396 of file resource_set.py.

7.121.2 Member Data Documentation

7.121.2.1 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.

7.121.2.2 rpki::resource_set.resource_set_ipv4::range_type = resource_range_ipv4 [static]

Type of range underlying this type of [resource_set](#).

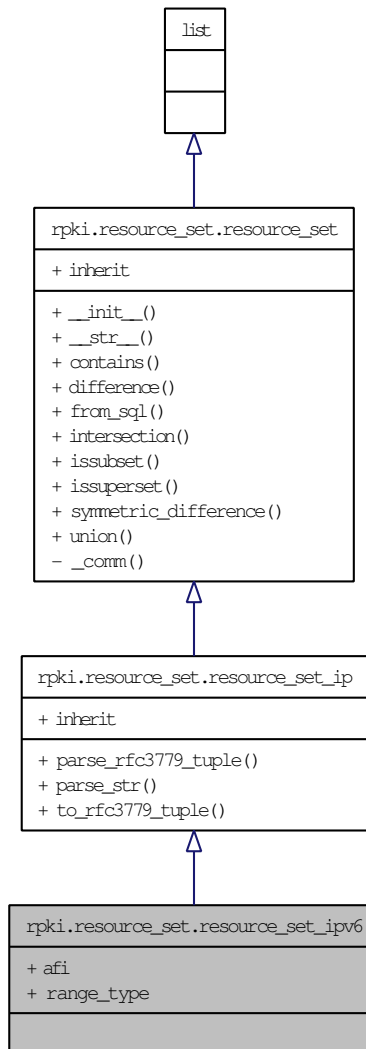
Definition at line 402 of file resource_set.py.

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

- [resource_set.py](#) (1873)

7.122 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](#).

7.122.1 Detailed Description

IPv6 address resource set.

Definition at line 409 of file resource_set.py.

7.122.2 Member Data Documentation

7.122.2.1 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.

7.122.2.2 rpki::resource_set.resource_set_ipv6::range_type = resource_range_ipv6 [static]

Type of range underlying this type of [resource_set](#).

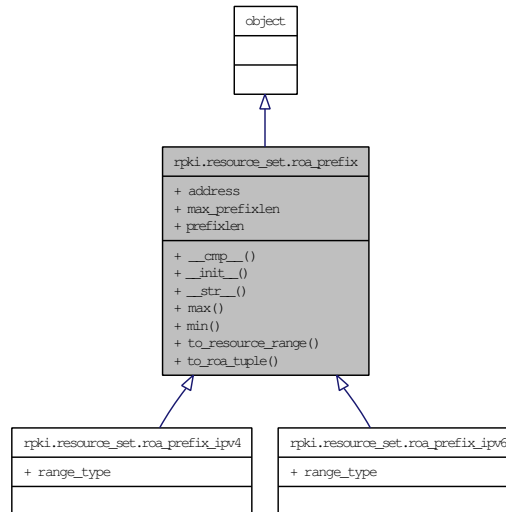
Definition at line 415 of file resource_set.py.

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

- [resource_set.py](#) (1873)

7.123 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](#)
Maximum prefix length.
- [prefixlen](#)
(Minimum) prefix length.

7.123.1 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`.

7.123.2 Member Function Documentation

7.123.2.1 `def rpki.resource_set.roa_prefix.__cmp__(self, other)`

Compare two ROA prefix objects. Comparison is based on address, prefixlen, and max_prefixlen, in that order.

Definition at line 586 of file `resource_set.py`.

7.123.2.2 `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`.

7.123.2.3 `def rpki.resource_set.roa_prefix.__str__(self)`

Convert a ROA prefix to string format.

Definition at line 598 of file `resource_set.py`.

7.123.2.4 `def rpki.resource_set.roa_prefix.max(self)`

Return highest address covered by prefix.

Definition at line 616 of file `resource_set.py`.

7.123.2.5 `def rpki.resource_set.roa_prefix.min(self)`

Return lowest address covered by prefix.

Definition at line 612 of file `resource_set.py`.

7.123.2.6 def rpki.resource_set.roa_prefix.to_resource_range (self)

Convert this ROA prefix to the equivalent resource_range_ip object. This is an irreversible transformation because it loses the max_prefixlen attribute, nothing we can do about that.

Definition at line 605 of file resource_set.py.

7.123.2.7 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.

7.123.3 Member Data Documentation

7.123.3.1 rpki::resource_set.roa_prefix::address

Address portion of prefix.

Definition at line 582 of file resource_set.py.

7.123.3.2 rpki::resource_set.roa_prefix::max_prefixlen

Maximum prefix length.

Definition at line 584 of file resource_set.py.

7.123.3.3 rpki::resource_set.roa_prefix::prefixlen

(Minimum) prefix length.

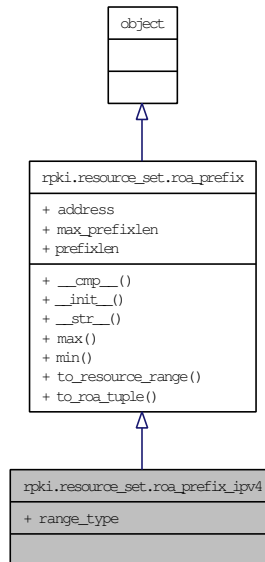
Definition at line 583 of file resource_set.py.

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

- [resource_set.py \(1873\)](#)

7.124 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](#).

7.124.1 Detailed Description

IPv4 ROA prefix.

Definition at line 626 of file resource_set.py.

7.124.2 Member Data Documentation

7.124.2.1 rpki::resource_set.roa_prefix_ipv4::range_type = resource_range_ipv4 [static]

Type of corresponding [resource_range_ip](#).

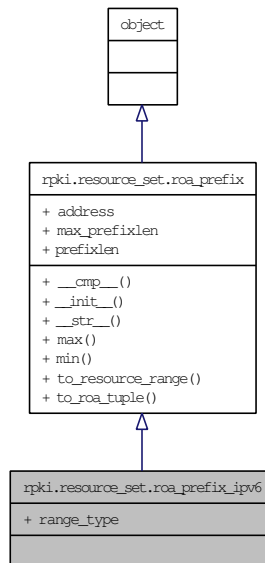
Definition at line 632 of file resource_set.py.

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

- [resource_set.py \(1873\)](#)

7.125 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*.

7.125.1 Detailed Description

IPv6 ROA prefix.

Definition at line 634 of file `resource_set.py`.

7.125.2 Member Data Documentation

7.125.2.1 rpki::resource_set.roa_prefix_ipv6::range_type = resource_range_ipv6 [static]

Type of corresponding [resource_range_ip](#).

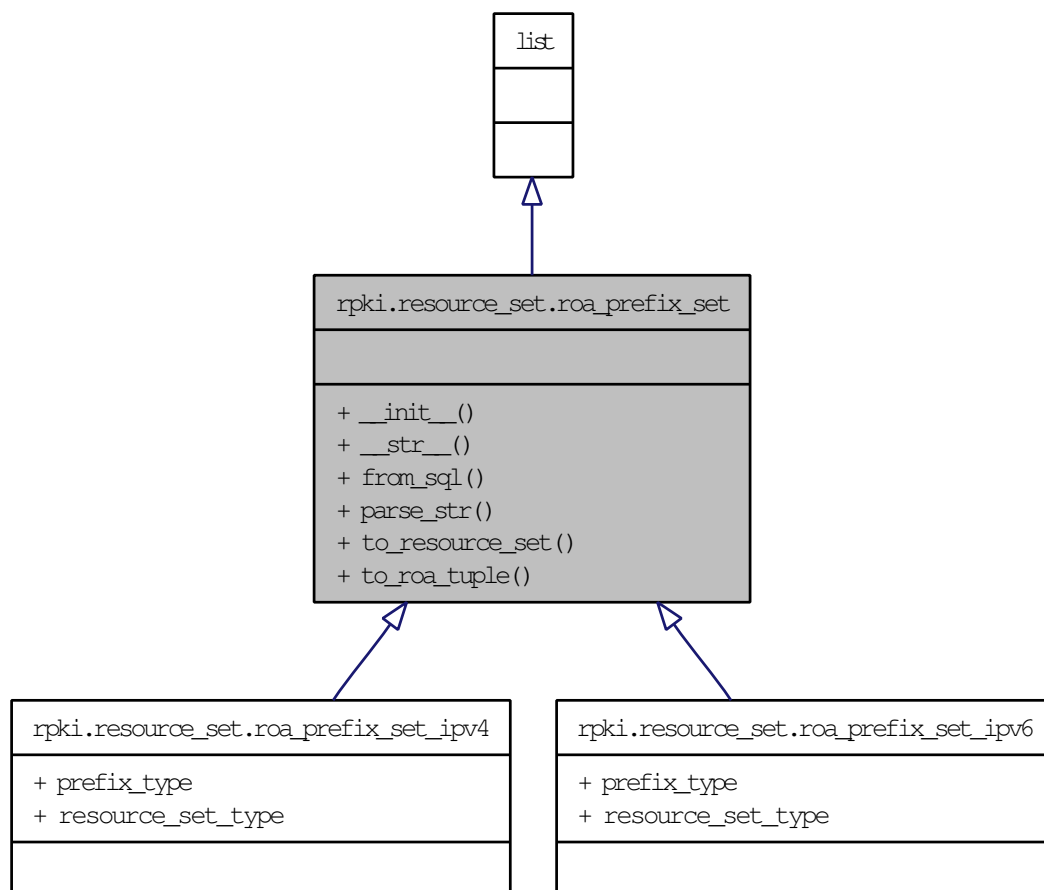
Definition at line 640 of file resource_set.py.

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

- [resource_set.py](#) (1873)

7.126 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](#)

7.126.1 Detailed Description

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

Definition at line 642 of file `resource_set.py`.

7.126.2 Member Function Documentation

7.126.2.1 `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`.

7.126.2.2 `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`.

7.126.2.3 `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`.

7.126.2.4 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.

7.126.2.5 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.

7.126.2.6 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.

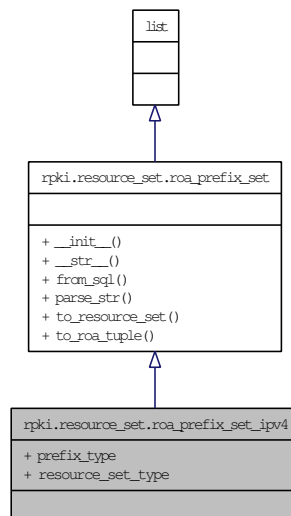
Definition at line 693 of file resource_set.py.

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

- [resource_set.py \(1873\)](#)

7.127 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.

7.127.1 Detailed Description

Set of IPv4 ROA prefixes.

Definition at line 701 of file `resource_set.py`.

7.127.2 Member Data Documentation

7.127.2.1 `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`.

7.127.2.2 `rpki::resource_set.roa_prefix_set_ipv4::resource_set_type = resource_set_ipv4` [static]

Type of corresponding [resource_set_ip](#) class.

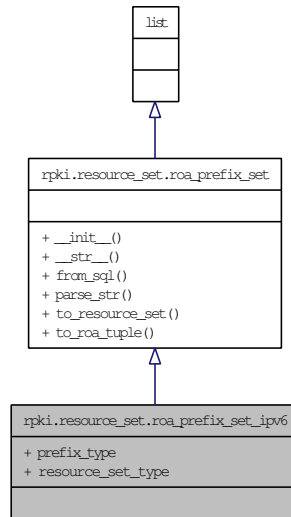
Definition at line 712 of file `resource_set.py`.

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

- [resource_set.py \(1873\)](#)

7.128 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.

7.128.1 Detailed Description

Set of IPv6 ROA prefixes.

Definition at line 714 of file `resource_set.py`.

7.128.2 Member Data Documentation

7.128.2.1 `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`.

7.128.2.2 rpki::resource_set.roa_prefix_set_ipv6::resource_set_type = resource_set_ipv6 [static]

Type of corresponding [resource_set_ip](#) class.

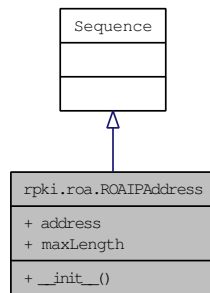
Definition at line 725 of file resource_set.py.

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

- [resource_set.py \(1873\)](#)

7.129 rpki.roa.ROAIPAddress Class Reference

Inheritance diagram for rpki.roa.ROAIPAddress:



Public Member Functions

- `def __init__`

Public Attributes

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

7.129.1 Detailed Description

Definition at line 65 of file roa.py.

7.129.2 Member Function Documentation

7.129.2.1 `def rpki.roa.ROAIPAddress.__init__(self, optional = 0, default = '')`

Definition at line 66 of file roa.py.

7.129.3 Member Data Documentation

7.129.3.1 rpki.roa.ROAIPAddress.address

Definition at line 67 of file roa.py.

7.129.3.2 rpki.roa.ROAIPAddress.maxLength

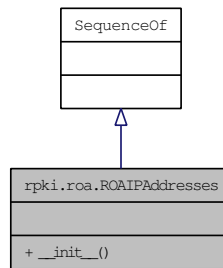
Definition at line 68 of file roa.py.

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

- [roa.py \(1873\)](#)

7.130 rpki.roa.ROAIPAddresses Class Reference

Inheritance diagram for rpki.roa.ROAIPAddresses:



Public Member Functions

- [def __init__](#)

7.130.1 Detailed Description

Definition at line 72 of file roa.py.

7.130.2 Member Function Documentation

7.130.2.1 def rpki.roa.ROAIPAddresses.__init__ (self, optional = 0, default = ")

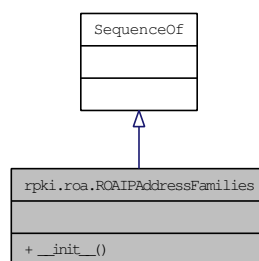
Definition at line 73 of file roa.py.

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

- [roa.py \(1873\)](#)

7.131 rpki.roa.ROAIPAddressFamilies Class Reference

Inheritance diagram for rpki.roa.ROAIPAddressFamilies:



Public Member Functions

- `def __init__`

7.131.1 Detailed Description

Definition at line 83 of file roa.py.

7.131.2 Member Function Documentation

7.131.2.1 `def rpki.roa.ROAIPAddressFamilies.__init__ (self, optional = 0, default = "")`

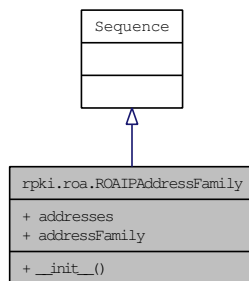
Definition at line 84 of file roa.py.

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

- [roa.py \(1873\)](#)

7.132 rpki.roa.ROAIPAddressFamily Class Reference

Inheritance diagram for rpki.roa.ROAIPAddressFamily:



Public Member Functions

- [def __init__](#)

Public Attributes

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

7.132.1 Detailed Description

Definition at line 76 of file roa.py.

7.132.2 Member Function Documentation

7.132.2.1 `def rpki.roa.ROAIPAddressFamily.__init__(self, optional = 0, default = "")`

Definition at line 77 of file roa.py.

7.132.3 Member Data Documentation

7.132.3.1 `rpki.roa.ROAIPAddressFamily.addresses`

Definition at line 79 of file roa.py.

7.132.3.2 rpki.roa.ROAIPAddressFamily.addressFamily

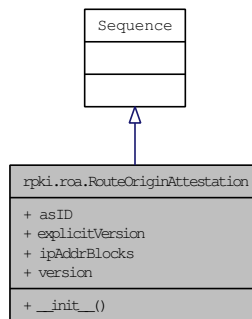
Definition at line 78 of file roa.py.

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

- [roa.py \(1873\)](#)

7.133 rpki.roa.RouteOriginAttestation Class Reference

Inheritance diagram for rpki.roa.RouteOriginAttestation:



Public Member Functions

- `def __init__`

Public Attributes

- `asID`
- `explicitVersion`
- `ipAddrBlocks`
- `version`

7.133.1 Detailed Description

Definition at line 87 of file roa.py.

7.133.2 Member Function Documentation

7.133.2.1 `def rpki.roa.RouteOriginAttestation.__init__ (self, optional = 0, default = "")`

Definition at line 88 of file roa.py.

7.133.3 Member Data Documentation

7.133.3.1 rpki.roa.RouteOriginAttestation.asID

Definition at line 91 of file roa.py.

7.133.3.2 rpki.roa.RouteOriginAttestation.explicitVersion

Definition at line 90 of file roa.py.

7.133.3.3 rpki.roa.RouteOriginAttestation.ipAddrBlocks

Definition at line 92 of file roa.py.

7.133.3.4 rpki.roa.RouteOriginAttestation.version

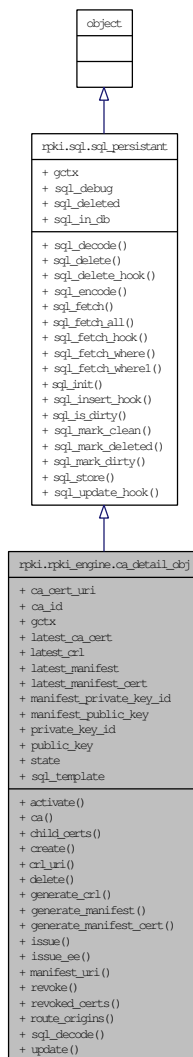
Definition at line 89 of file roa.py.

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

- [roa.py \(1873\)](#)

7.134 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](#)

7.134.1 Detailed Description

Internal CA detail object.

Definition at line 332 of file `rpki_engine.py`.

7.134.2 Member Function Documentation

7.134.2.1 `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.

7.134.2.2 `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.

7.134.2.3 `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.

7.134.2.4 `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.

7.134.2.5 `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.

7.134.2.6 `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.

7.134.2.7 `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.

7.134.2.8 `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.

7.134.2.9 `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.

7.134.2.10 `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.

7.134.2.11 `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.

7.134.2.12 `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.

7.134.2.13 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.

7.134.2.14 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.

7.134.2.15 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.

7.134.2.16 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_persistent](#).

Definition at line 350 of file rpki_engine.py.

7.134.2.17 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.

7.134.3 Member Data Documentation

7.134.3.1 rpki.rpki_engine.ca_detail_obj.ca_cert_uri

Definition at line 386 of file rpki_engine.py.

7.134.3.2 rpki.rpki_engine.ca_detail_obj.ca_id

Definition at line 491 of file rpki_engine.py.

7.134.3.3 rpki.rpki_engine.ca_detail_obj.gctx

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

Definition at line 490 of file rpki_engine.py.

7.134.3.4 rpki.rpki_engine.ca_detail_obj.latest_ca_cert

Definition at line 385 of file rpki_engine.py.

7.134.3.5 rpki.rpki_engine.ca_detail_obj.latest_crl

Definition at line 594 of file rpki_engine.py.

7.134.3.6 rpki.rpki_engine.ca_detail_obj.latest_manifest

Definition at line 619 of file rpki_engine.py.

7.134.3.7 rpki.rpki_engine.ca_detail_obj.latest_manifest_cert

Definition at line 463 of file rpki_engine.py.

7.134.3.8 rpki.rpki_engine.ca_detail_obj.manifest_private_key_id

Definition at line 461 of file rpki_engine.py.

7.134.3.9 rpki.rpki_engine.ca_detail_obj.manifest_public_key

Definition at line 462 of file rpki_engine.py.

7.134.3.10 rpki.rpki_engine.ca_detail_obj.private_key_id

Definition at line 460 of file rpki_engine.py.

7.134.3.11 rpki.rpki_engine.ca_detail_obj.public_key

Definition at line 496 of file rpki_engine.py.

7.134.3.12 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.

7.134.3.13 rpki.rpki_engine.ca_detail_obj.state

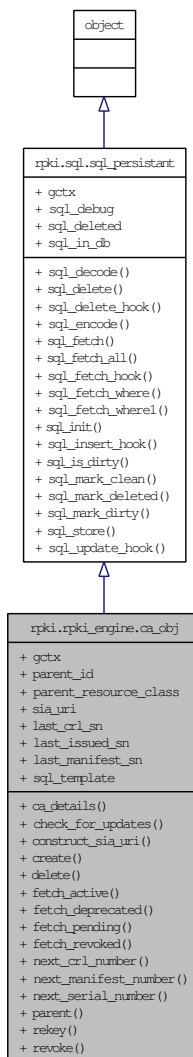
Definition at line 390 of file rpki_engine.py.

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

- [rpki_engine.py \(1873\)](#)

7.135 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](#)

7.135.1 Detailed Description

Internal CA object.

Definition at line 160 of file rpki_engine.py.

7.135.2 Member Function Documentation

7.135.2.1 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.

7.135.2.2 def rpki.rpki_engine.ca_obj.check_for_updates (*self*, *parent*, *rc*)

Parent has signaled continued existence of a resource class we already knew about, so we need to check for an updated certificate, changes in resource coverage, revocation and reissue with the same key, etc.

Definition at line 213 of file rpki_engine.py.

7.135.2.3 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.

7.135.2.4 def rpki.rpki_engine.ca_obj.create (*cls*, *parent*, *rc*)

Parent has signaled existence 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.

7.135.2.5 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.

7.135.2.6 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.

7.135.2.7 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.

7.135.2.8 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.

7.135.2.9 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.

7.135.2.10 def rpki.rpki_engine.ca_obj.next_crl_number (self)

Allocate a CRL serial number.

Definition at line 296 of file rpki_engine.py.

7.135.2.11 def rpki.rpki_engine.ca_obj.next_manifest_number (self)

Allocate a manifest serial number.

Definition at line 290 of file rpki_engine.py.

7.135.2.12 def rpki.rpki_engine.ca_obj.next_serial_number (self)

Allocate a certificate serial number.

Definition at line 284 of file rpki_engine.py.

7.135.2.13 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.

7.135.2.14 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.

7.135.2.15 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.

7.135.3 Member Data Documentation**7.135.3.1 rpki.rpki_engine.ca_obj.gctx**

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

Definition at line 253 of file rpki_engine.py.

7.135.3.2 int rpki.rpki_engine.ca_obj.last_crl_sn = 0 [static]

Definition at line 172 of file rpki_engine.py.

7.135.3.3 int rpki.rpki_engine.ca_obj.last_issued_sn = 0 [static]

Definition at line 173 of file rpki_engine.py.

7.135.3.4 int rpki.rpki_engine.ca_obj.last_manifest_sn = 0 [static]

Definition at line 174 of file rpki_engine.py.

7.135.3.5 rpki.rpki_engine.ca_obj.parent_id

Definition at line 254 of file rpki_engine.py.

7.135.3.6 rpki.rpki_engine.ca_obj.parent_resource_class

Definition at line 255 of file rpki_engine.py.

7.135.3.7 rpki.rpki_engine.ca_obj.sia_uri

Definition at line 223 of file rpki_engine.py.

7.135.3.8 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")
```

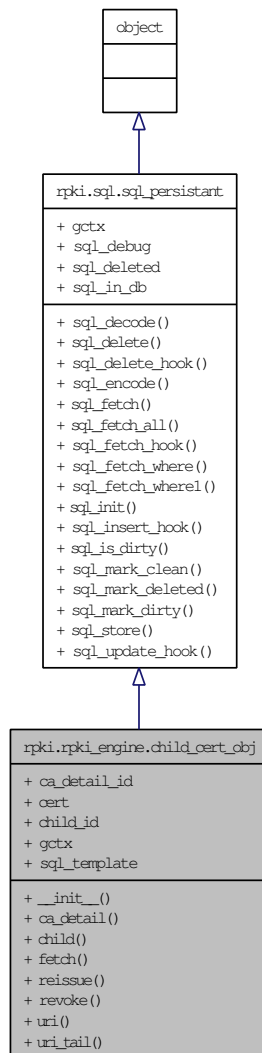
Definition at line 163 of file rpki_engine.py.

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

- [rpki_engine.py \(1873\)](#)

7.136 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](#)

7.136.1 Detailed Description

Certificate that has been issued to a child.

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

7.136.2 Member Function Documentation

7.136.2.1 `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`.

7.136.2.2 `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`.

7.136.2.3 `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`.

7.136.2.4 `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.

7.136.2.5 `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.

7.136.2.6 `def rpki.rpki_engine.child_cert_obj.revoke (self)`

Revoke a child cert.

Definition at line 665 of file rpki_engine.py.

7.136.2.7 `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.

7.136.2.8 `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.

7.136.3 Member Data Documentation

7.136.3.1 `rpki.rpki_engine.child_cert_obj.ca_detail_id`

Definition at line 644 of file rpki_engine.py.

7.136.3.2 rpki.rpki_engine.child_cert_obj.cert

Definition at line 645 of file rpki_engine.py.

7.136.3.3 rpki.rpki_engine.child_cert_obj.child_id

Definition at line 643 of file rpki_engine.py.

7.136.3.4 rpki.rpki_engine.child_cert_obj.gctx

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

Definition at line 642 of file rpki_engine.py.

7.136.3.5 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")
```

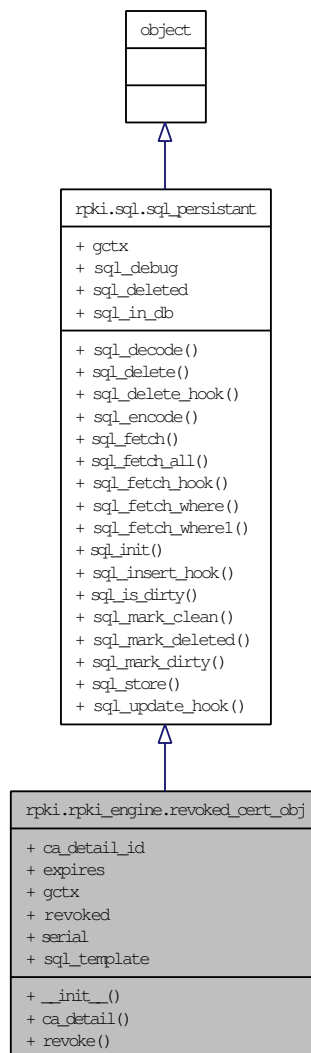
Definition at line 632 of file rpki_engine.py.

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

- [rpki_engine.py \(1873\)](#)

7.137 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](#)

7.137.1 Detailed Description

Tombstone for a revoked certificate.

Definition at line 761 of file `rpki_engine.py`.

7.137.2 Member Function Documentation

7.137.2.1 `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`.

7.137.2.2 `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`.

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

Revoke a certificate.

Definition at line 787 of file `rpki_engine.py`.

7.137.3 Member Data Documentation

7.137.3.1 rpki.rpki_engine.revoked_cert_obj.ca_detail_id

Definition at line 778 of file rpki_engine.py.

7.137.3.2 rpki.rpki_engine.revoked_cert_obj.expires

Definition at line 777 of file rpki_engine.py.

7.137.3.3 rpki.rpki_engine.revoked_cert_obj.gctx

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

Definition at line 774 of file rpki_engine.py.

7.137.3.4 rpki.rpki_engine.revoked_cert_obj.revoked

Definition at line 776 of file rpki_engine.py.

7.137.3.5 rpki.rpki_engine.revoked_cert_obj.serial

Definition at line 775 of file rpki_engine.py.

7.137.3.6 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))
```

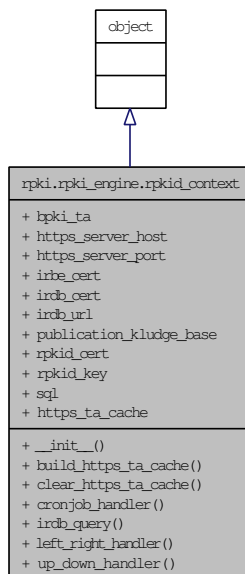
Definition at line 764 of file rpki_engine.py.

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

- [rpki_engine.py \(1873\)](#)

7.138 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.

7.138.1 Detailed Description

A container for various global rpkid parameters.

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

7.138.2 Member Function Documentation

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

Definition at line 27 of file `rpki_engine.py`.

7.138.2.2 `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`.

7.138.2.3 `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`.

7.138.2.4 `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`.

7.138.2.5 `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.

7.138.2.6 `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.

7.138.2.7 `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.

7.138.3 Member Data Documentation**7.138.3.1** `rpki.rpki_engine.rpkid_context.bpki_ta`

Definition at line 31 of file rpki_engine.py.

7.138.3.2 `rpki.rpki_engine.rpkid_context.https_server_host`

Definition at line 39 of file rpki_engine.py.

7.138.3.3 `rpki.rpki_engine.rpkid_context.https_server_port`

Definition at line 40 of file rpki_engine.py.

7.138.3.4 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.

7.138.3.5 rpki.rpki_engine.rpkid_context.irbe_cert

Definition at line 33 of file rpki_engine.py.

7.138.3.6 rpki.rpki_engine.rpkid_context.irdb_cert

Definition at line 32 of file rpki_engine.py.

7.138.3.7 rpki.rpki_engine.rpkid_context.irdb_url

Definition at line 37 of file rpki_engine.py.

7.138.3.8 rpki.rpki_engine.rpkid_context.publication_kludge_base

Definition at line 42 of file rpki_engine.py.

7.138.3.9 rpki.rpki_engine.rpkid_context.rpkid_cert

Definition at line 34 of file rpki_engine.py.

7.138.3.10 rpki.rpki_engine.rpkid_context.rpkid_key

Definition at line 35 of file rpki_engine.py.

7.138.3.11 rpki.rpki_engine.rpkid_context.sql

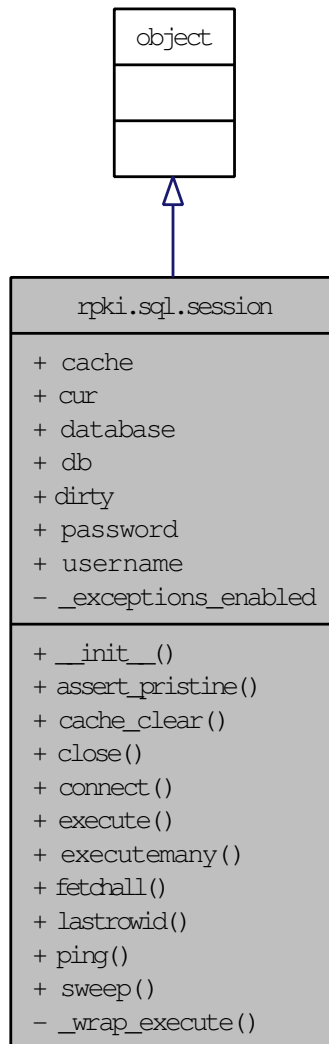
Definition at line 29 of file rpki_engine.py.

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

- [rpki_engine.py \(1873\)](#)

7.139 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

7.139.1 Detailed Description

SQL session layer.

Definition at line 23 of file sql.py.

7.139.2 Member Function Documentation

7.139.2.1 def rpki.sql.session.__init__ (*self*, *cfg*)

Definition at line 28 of file sql.py.

7.139.2.2 def rpki.sql.session._wrap_execute (*self*, *func*, *query*, *args*) [private]

Definition at line 58 of file sql.py.

7.139.2.3 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.

7.139.2.4 def rpki.sql.session.cache_clear (self)

Clear the object cache.

Definition at line 78 of file sql.py.

7.139.2.5 def rpki.sql.session.close (self)

Definition at line 47 of file sql.py.

7.139.2.6 def rpki.sql.session.connect (self)

Definition at line 43 of file sql.py.

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

Definition at line 66 of file sql.py.

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

Definition at line 69 of file sql.py.

7.139.2.9 def rpki.sql.session.fetchall (self)

Definition at line 72 of file sql.py.

7.139.2.10 def rpki.sql.session.lastrowid (self)

Definition at line 75 of file sql.py.

7.139.2.11 def rpki.sql.session.ping (self)

Definition at line 55 of file sql.py.

7.139.2.12 def rpki.sql.session.sweep (self)

Write any dirty objects out to SQL.

Definition at line 86 of file sql.py.

7.139.3 Member Data Documentation

7.139.3.1 **rpki.sql.session._exceptions_enabled = False** `[static, private]`

Definition at line 26 of file sql.py.

7.139.3.2 **rpki.sql.session.cache**

Definition at line 38 of file sql.py.

7.139.3.3 **rpki.sql.session.cur**

Definition at line 45 of file sql.py.

7.139.3.4 **rpki.sql.session.database**

Definition at line 35 of file sql.py.

7.139.3.5 **rpki.sql.session.db**

Definition at line 44 of file sql.py.

7.139.3.6 **rpki.sql.session.dirty**

Definition at line 39 of file sql.py.

7.139.3.7 **rpki.sql.session.password**

Definition at line 36 of file sql.py.

7.139.3.8 **rpki.sql.session.username**

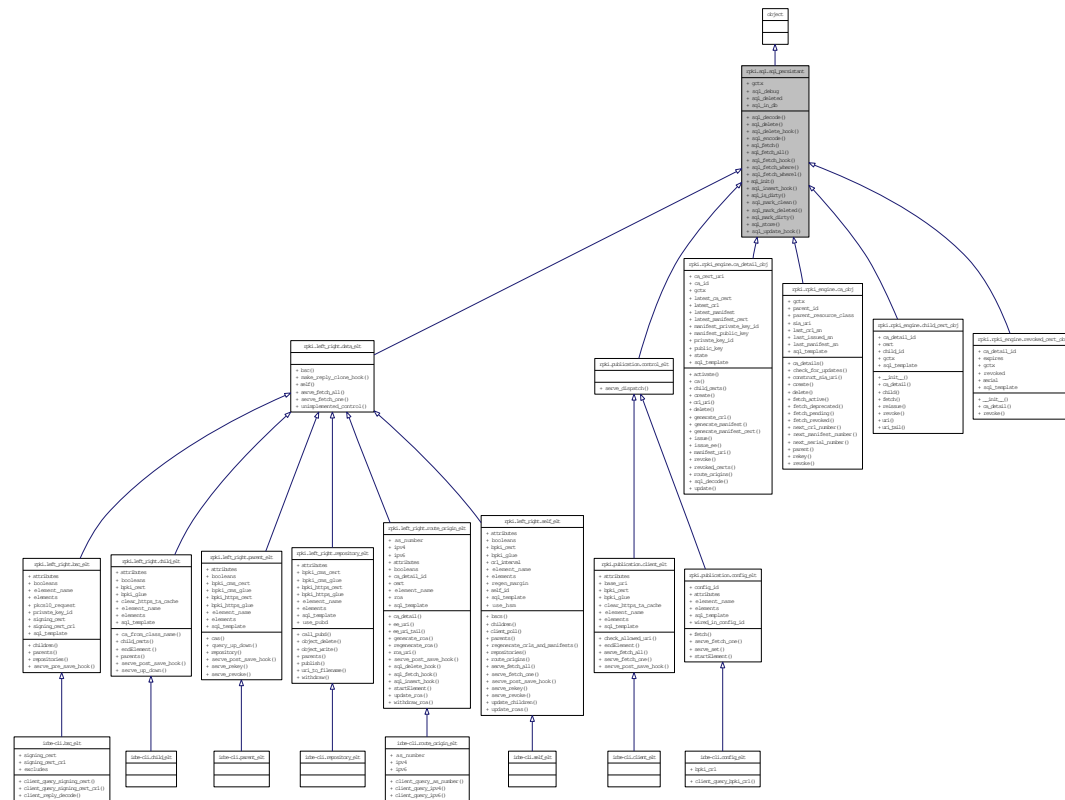
Definition at line 34 of file sql.py.

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

- [sql.py \(1873\)](#)

7.140 rpki.sql.sql_persistent Class Reference

Inheritance diagram for rpkgi.sql.sql_persistent:



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.

7.140.1 Detailed Description

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

Definition at line 115 of file sql.py.

7.140.2 Member Function Documentation

7.140.2.1 def rpki.sql.sql_persistent.sql_decode (*self*, *vals*)

Initialize an object with values returned by `self.sql_fetch()`. This is a default version that assumes a one-to-one mapping between column names in SQL and attribute names in Python. If you need something fancier, override this.

Reimplemented in [rpki.rpki_engine.ca_detail_obj](#).

Definition at line 262 of file sql.py.

7.140.2.2 def rpkgi.sql.sql_persistent.sql_delete (self)

Delete this object from SQL.

Definition at line 238 of file sql.py.

7.140.2.3 def rpkgi.sql.sql_persistent.sql_delete_hook (self)

Customization hook.

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

Definition at line 287 of file sql.py.

7.140.2.4 def rpkgi.sql.sql_persistent.sql_encode (self)

Convert object attributes into a dict for use with canned SQL queries. This is a default version that assumes a one-to-one mapping between column names in SQL and attribute names in Python. If you need something fancier, override this.

Definition at line 250 of file sql.py.

7.140.2.5 def rpkgi.sql.sql_persistent.sql_fetch (cls, gctx, id)

Fetch one object from SQL, based on its primary key.

Since in this one case we know that the primary index is also the cache key, we check for a cache hit directly in the hope of bypassing the SQL lookup entirely.

This method is usually called via a one-line class-specific wrapper. As a convenience, we also accept an id of None, and just return None in this case.

Definition at line 135 of file sql.py.

7.140.2.6 def rpkgi.sql.sql_persistent.sql_fetch_all (cls, gctx)

Fetch all objects of this type from SQL.

Definition at line 170 of file sql.py.

7.140.2.7 `def rpki.sql.sql_persistent.sql_fetch_hook (self)`

Customization hook.

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

Definition at line 274 of file sql.py.

7.140.2.8 `def rpki.sql.sql_persistent.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.

7.140.2.9 `def rpki.sql.sql_persistent.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.

7.140.2.10 `def rpki.sql.sql_persistent.sql_init (cls, gctx, row, key)`

Initialize one Python object from the result of a SQL query.

Definition at line 197 of file sql.py.

7.140.2.11 `def rpki.sql.sql_persistent.sql_insert_hook (self)`

Customization hook.

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

Definition at line 278 of file sql.py.

7.140.2.12 `def rpki.sql.sql_persistent.sql_is_dirty (self)`

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

Definition at line 215 of file sql.py.

7.140.2.13 def rpki.sql.sql_persistent.sql_mark_clean (self)

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

Definition at line 211 of file sql.py.

7.140.2.14 def rpki.sql.sql_persistent.sql_mark_deleted (self)

Mark this object as needing to be deleted in SQL.

Definition at line 219 of file sql.py.

7.140.2.15 def rpki.sql.sql_persistent.sql_mark_dirty (self)

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

Definition at line 207 of file sql.py.

7.140.2.16 def rpki.sql.sql_persistent.sql_store (self)

Store this object to SQL.

Definition at line 223 of file sql.py.

7.140.2.17 def rpki.sql.sql_persistent.sql_update_hook (self)

Customization hook.

Definition at line 282 of file sql.py.

7.140.3 Member Data Documentation**7.140.3.1 rpki.sql.sql_persistent.gctx**

Reimplemented in [rpki.rpki_engine.ca_obj](#), [rpki.rpki_engine.ca_detail_obj](#), [rpki.rpki_engine.child_cert_obj](#), and [rpki.rpki_engine.revoked_cert_obj](#).

Definition at line 200 of file sql.py.

7.140.3.2 rpki::sql.sql_persistent::sql_debug = False [static]

Enable logging of SQL actions.

Definition at line 132 of file sql.py.

7.140.3.3 rpki::sql.sql_persistent::sql_deleted = False [static]

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

Definition at line 127 of file sql.py.

7.140.3.4 rpki::sql.sql_persistent::sql_in_db = False [static]

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

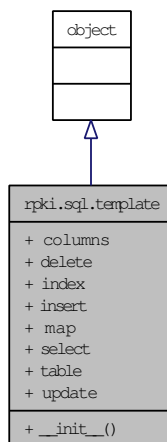
Definition at line 122 of file sql.py.

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

- [sql.py](#) (1873)

7.141 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](#)

7.141.1 Detailed Description

SQL template generator.

Definition at line 96 of file sql.py.

7.141.2 Member Function Documentation

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

Build a SQL template.

Definition at line 98 of file sql.py.

7.141.3 Member Data Documentation

7.141.3.1 rpki.sql.template.columns

Definition at line 105 of file sql.py.

7.141.3.2 rpki.sql.template.delete

Definition at line 113 of file sql.py.

7.141.3.3 rpki.sql.template.index

Definition at line 104 of file sql.py.

7.141.3.4 rpki.sql.template.insert

Definition at line 108 of file sql.py.

7.141.3.5 rpki.sql.template.map

Definition at line 106 of file sql.py.

7.141.3.6 rpki.sql.template.select

Definition at line 107 of file sql.py.

7.141.3.7 rpki.sql.template.table

Definition at line 103 of file sql.py.

7.141.3.8 rpki.sql.template.update

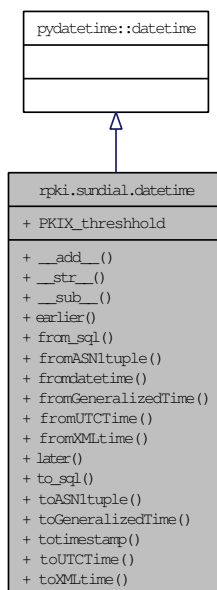
Definition at line 110 of file sql.py.

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

- [sql.py \(1873\)](#)

7.142 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_threshold](#) = pydatetime.datetime(2050, 1, 1)

Threshold specified in RFC 3280 for switchover from UTCTime to GeneralizedTime.

7.142.1 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.

7.142.2 Member Function Documentation

7.142.2.1 def rpki.sundial.datetime.__add__(self, other)

Force correct class for timedelta results.

Definition at line 102 of file sundial.py.

7.142.2.2 def rpki.sundial.datetime.__str__(self)

Definition at line 92 of file sundial.py.

7.142.2.3 def rpki.sundial.datetime.__sub__ (self, other)

Force correct class for timedelta results.

Definition at line 106 of file sundial.py.

7.142.2.4 def rpki.sundial.datetime.earlier (self, other)

Return the earlier of two timestamps.

Definition at line 133 of file sundial.py.

7.142.2.5 def rpki.sundial.datetime.from_sql (cls, x)

Convert from SQL storage format.

Definition at line 111 of file sundial.py.

7.142.2.6 def rpki.sundial.datetime.fromASN1tuple (cls, x)

Convert from ASN.1 tuple representation.

Definition at line 60 of file sundial.py.

7.142.2.7 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.

7.142.2.8 def rpki.sundial.datetime.fromGeneralizedTime (cls, x)

Convert from ASN.1 GeneralizedTime.

Definition at line 51 of file sundial.py.

7.142.2.9 def rpki.sundial.datetime.fromUTCTime (cls, x)

Convert from ASN.1 UTCTime.

Definition at line 42 of file sundial.py.

7.142.2.10 def rpki.sundial.datetime.fromXMLtime (cls, x)

Convert from XML time representation.

Definition at line 81 of file sundial.py.

7.142.2.11 def rpki.sundial.datetime.later (self, other)

Return the later of two timestamps.

Definition at line 129 of file sundial.py.

7.142.2.12 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.

7.142.2.13 def rpki.sundial.datetime.toASN1tuple (self)

Convert to ASN.1 tuple representation.

Definition at line 73 of file sundial.py.

7.142.2.14 def rpki.sundial.datetime.toGeneralizedTime (self)

Convert to ASN.1 GeneralizedTime.

Definition at line 55 of file sundial.py.

7.142.2.15 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.

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

Convert to ASN.1 UTCTime.

Definition at line 46 of file sundial.py.

7.142.2.17 def rpki.sundial.datetime.toXMLtime (*self*)

Convert to XML time representation.

Definition at line 88 of file sundial.py.

7.142.3 Member Data Documentation**7.142.3.1** rpki::sundial.datetime::PKIX_threshold = pydate-
time.datetime(2050, 1, 1) [static]

Threshold specified in RFC 3280 for switchover from UTCTime to GeneralizedTime.

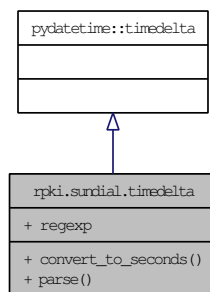
Definition at line 71 of file sundial.py.

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

- [sundial.py \(1873\)](#)

7.143 rpki.sundial.timedelta Class Reference

Inheritance diagram for rpki.sundial.timedelta:

**Public Member Functions**

- def [convert_to_seconds](#)
- def [parse](#)

Static Public Attributes

- tuple [regex](#)

Hideously ugly regular expression to parse the complex text form.

7.143.1 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.

7.143.2 Member Function Documentation

7.143.2.1 def rpki.sundial.timedelta.convert_to_seconds (self)

Convert a timedelta interval to seconds.

Definition at line 168 of file sundial.py.

7.143.2.2 def rpki.sundial.timedelta.parse (cls, arg)

Parse text into a timedelta object.

Definition at line 159 of file sundial.py.

7.143.3 Member Data Documentation

7.143.3.1 rpki::sundial.timedelta::regex [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)
```

Tags are intended for use with `re.MatchObject.groupdict()` and map directly to the keywords expected by the `timedelta` constructor.

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

- ## 7.144 rpki.up_down.base_elt Class Reference

[illegible]

- def `check_response`
- def `endElement`
- def `make_b64elt`
- def `make_elt`
- def `serve_pdu`
- def `startElement`

Generic PDU object.

Virtual class, just provides some default methods.

Definition at line 28 of file up_down.py.

7.144.2 Member Function Documentation

7.144.2.1 `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.

7.144.2.2 `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.

7.144.2.3 `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.

7.144.2.4 `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.

7.144.2.5 `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](#), [rpki.up_down.revoke_pdu](#), [rootd.list_pdu](#), [rootd.issue_pdu](#), and [rootd.revoke_pdu](#).

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

7.144.2.6 `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](#).

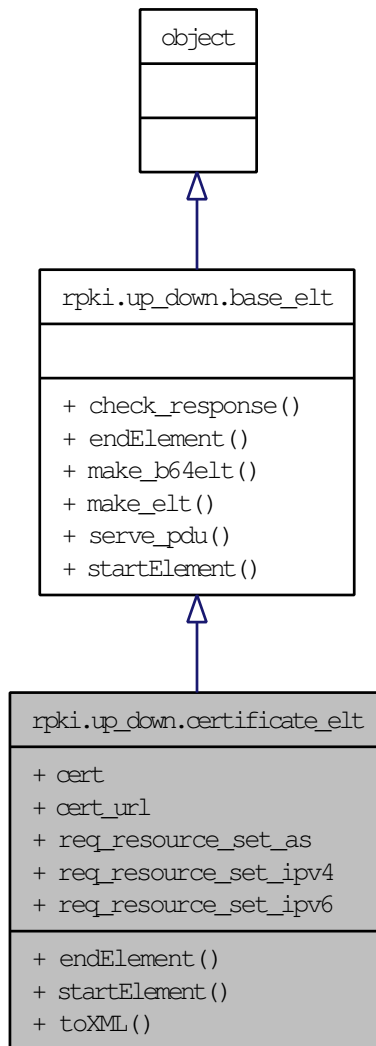
Definition at line 34 of file `up_down.py`.

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

- [up_down.py](#) (1873)

7.145 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](#)

7.145.1 Detailed Description

Up-Down protocol representation of an issued certificate.

Definition at line 99 of file up_down.py.

7.145.2 Member Function Documentation

7.145.2.1 `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.

7.145.2.2 `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.

7.145.2.3 `def rpki.up_down.certificate_elt.toXML (self)`

Generate a <certificate/> element.

Definition at line 116 of file up_down.py.

7.145.3 Member Data Documentation

7.145.3.1 `rpki.up_down.certificate_elt.cert`

Definition at line 113 of file up_down.py.

7.145.3.2 rpki.up_down.certificate_elt.cert_url

Definition at line 105 of file up_down.py.

7.145.3.3 rpki.up_down.certificate_elt.req_resource_set_as

Definition at line 106 of file up_down.py.

7.145.3.4 rpki.up_down.certificate_elt.req_resource_set_ipv4

Definition at line 107 of file up_down.py.

7.145.3.5 rpki.up_down.certificate_elt.req_resource_set_ipv6

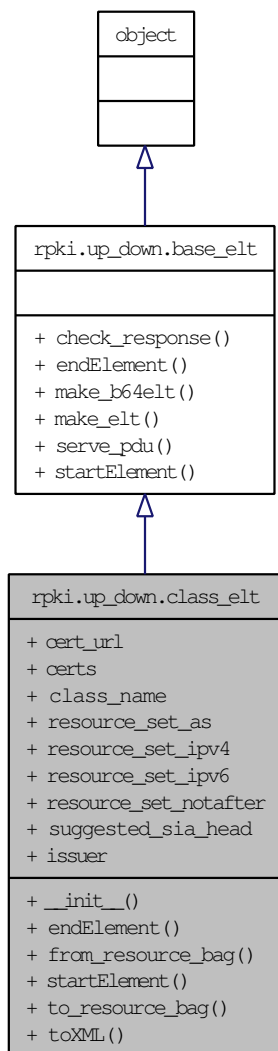
Definition at line 108 of file up_down.py.

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

- [up_down.py \(1873\)](#)

7.146 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

7.146.1 Detailed Description

Up-Down protocol representation of a resource class.

Definition at line 123 of file up_down.py.

7.146.2 Member Function Documentation

7.146.2.1 def rpki.up_down.class_elt.__init__ (*self*)

Initialize class_elt.

Definition at line 128 of file up_down.py.

7.146.2.2 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.

7.146.2.3 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.

7.146.2.4 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.

7.146.2.5 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.

7.146.2.6 def rpki.up_down.class_elt.toXML (self)

Generate a <class/> element.

Definition at line 157 of file up_down.py.

7.146.3 Member Data Documentation**7.146.3.1 rpki.up_down.class_elt.cert_url**

Definition at line 142 of file up_down.py.

7.146.3.2 rpki.up_down.class_elt.certs

Definition at line 130 of file up_down.py.

7.146.3.3 rpki.up_down.class_elt.class_name

Definition at line 141 of file up_down.py.

7.146.3.4 rpki.up_down.class_elt.issuer = None [static]

Definition at line 126 of file up_down.py.

7.146.3.5 rpki.up_down.class_elt.resource_set_as

Definition at line 144 of file up_down.py.

7.146.3.6 rpki.up_down.class_elt.resource_set_ipv4

Definition at line 145 of file up_down.py.

7.146.3.7 rpki.up_down.class_elt.resource_set_ipv6

Definition at line 146 of file up_down.py.

7.146.3.8 rpki.up_down.class_elt.resource_set_notafter

Definition at line 147 of file up_down.py.

7.146.3.9 rpki.up_down.class_elt.suggested_sia_head

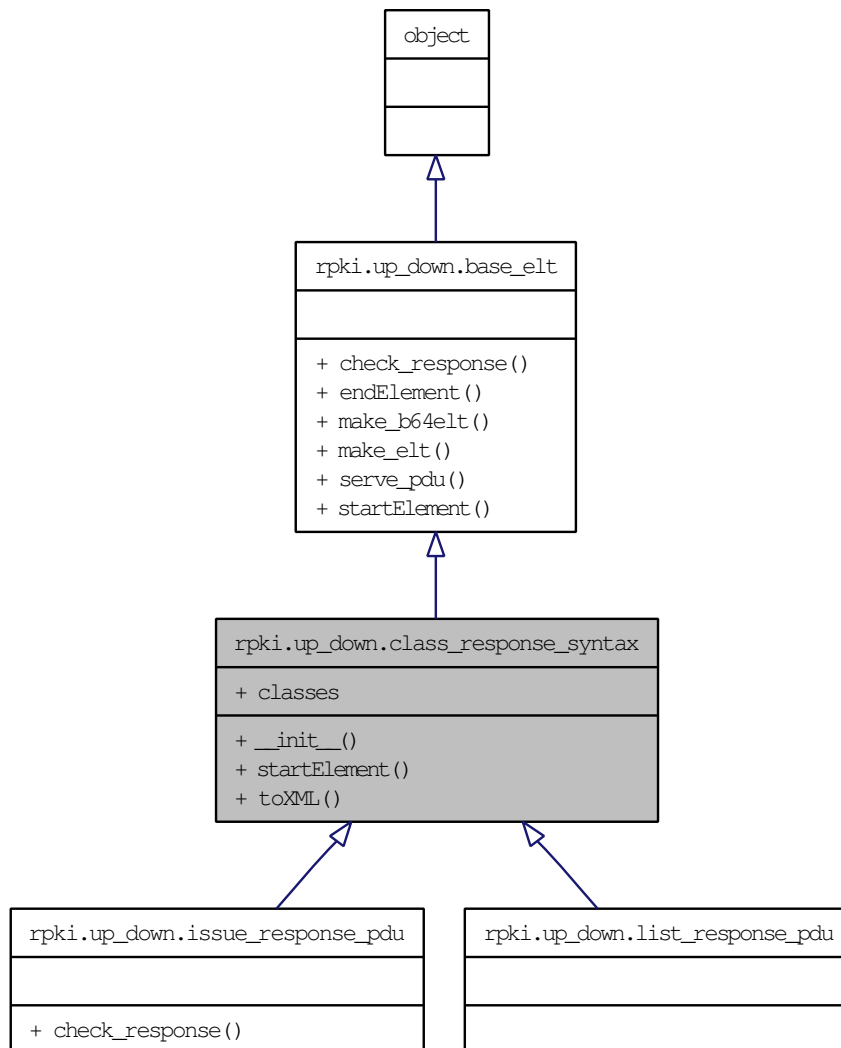
Definition at line 143 of file up_down.py.

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

- [up_down.py \(1873\)](#)

7.147 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](#)

7.147.1 Detailed Description

Syntax for Up-Down protocol "list_response" and "issue_response" PDUs.

Definition at line 220 of file up_down.py.

7.147.2 Member Function Documentation

7.147.2.1 def rpki.up_down.class_response_syntax.__init__ (self)

Initialize class_response_syntax.

Definition at line 223 of file up_down.py.

7.147.2.2 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.

7.147.2.3 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.

7.147.3 Member Data Documentation

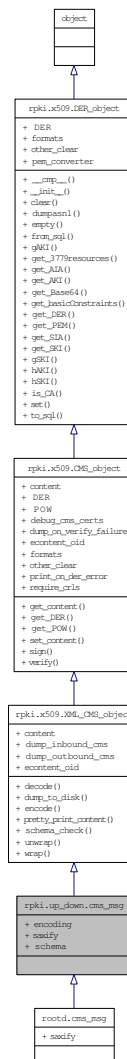
7.147.3.1 rpki.up_down.class_response_syntax.classes

Definition at line 225 of file up_down.py.

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

- [up_down.py](#) (1873)

Inheritance diagram for rpkgi.up_down.cms_msg:



- string **encoding** = "UTF-8"
- **saxify** = sax_handler.saxify
- **schema** = rpki.relaxng.up_down

7.148.1 Detailed Description

Class to hold a CMS-signed up-down PDU.

Definition at line 528 of file up_down.py.

7.148.2 Member Data Documentation

7.148.2.1 `string rpki.up_down.cms_msg.encoding = "UTF-8"` [static]

Definition at line 531 of file up_down.py.

7.148.2.2 `rpki.up_down.cms_msg.saxify = sax_handler.saxify` [static]

Reimplemented in [rootd.cms_msg](#).

Definition at line 533 of file up_down.py.

7.148.2.3 `rpki.up_down.cms_msg.schema = rpki.relaxng.up_down` [static]

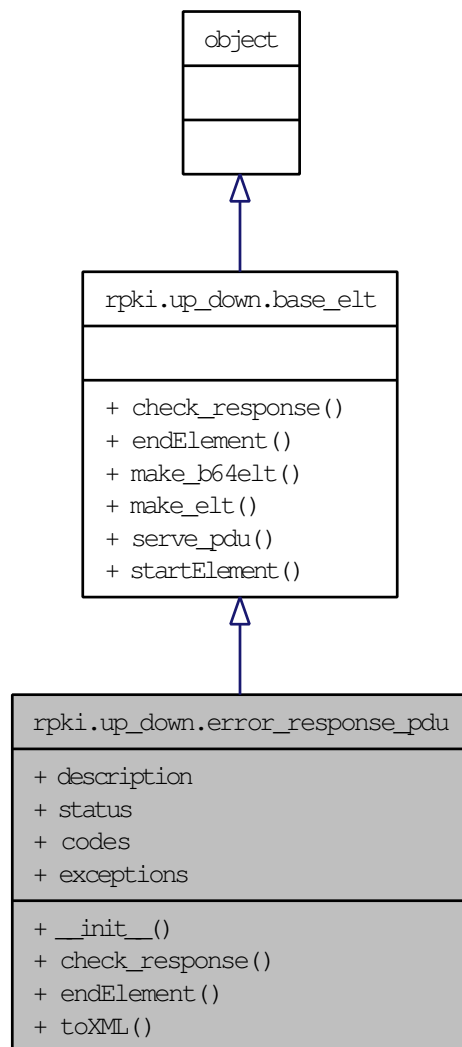
Definition at line 532 of file up_down.py.

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

- [up_down.py](#) (1873)

7.149 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](#) = { }

7.149.1 Detailed Description

Up-Down protocol "error_response" PDU.

Definition at line 389 of file up_down.py.

7.149.2 Member Function Documentation

7.149.2.1 `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.

7.149.2.2 `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.

7.149.2.3 `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.

7.149.2.4 def rpki.up_down.error_response_pdu.toXML (self)

Generate payload of "error_response" PDU.

Definition at line 428 of file up_down.py.

7.149.3 Member Data Documentation

7.149.3.1 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.

7.149.3.2 rpki.up_down.error_response_pdu.description

Definition at line 412 of file up_down.py.

7.149.3.3 dictionary rpki.up_down.error_response_pdu.exceptions = {} [static]

Definition at line 403 of file up_down.py.

7.149.3.4 rpki.up_down.error_response_pdu.status

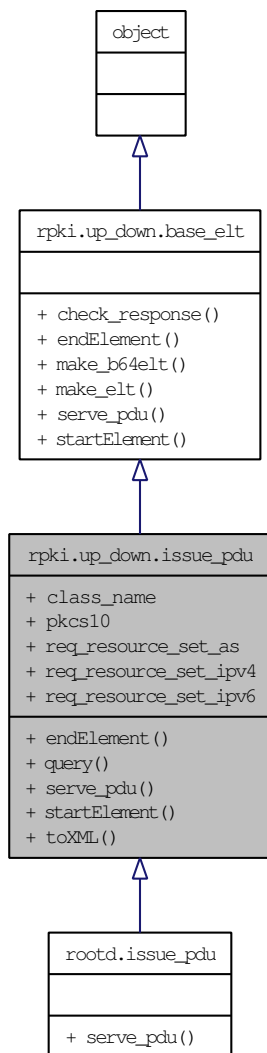
Definition at line 409 of file up_down.py.

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

- [up_down.py \(1873\)](#)

7.150 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](#)

7.150.1 Detailed Description

Up-Down protocol "issue" PDU.

Definition at line 244 of file up_down.py.

7.150.2 Member Function Documentation

7.150.2.1 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.

7.150.2.2 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.

7.150.2.3 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](#).

Reimplemented in [rootd.issue_pdu](#).

Definition at line 268 of file up_down.py.

7.150.2.4 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.

7.150.2.5 def rpki.up_down.issue_pdu.toXML (*self*)

Generate payload of "issue" PDU.

Definition at line 261 of file up_down.py.

7.150.3 Member Data Documentation

7.150.3.1 rpki.up_down.issue_pdu.class_name

Definition at line 250 of file up_down.py.

7.150.3.2 rpki.up_down.issue_pdu.pkcs10

Definition at line 258 of file up_down.py.

7.150.3.3 rpki.up_down.issue_pdu.req_resource_set_as

Definition at line 251 of file up_down.py.

7.150.3.4 rpki.up_down.issue_pdu.req_resource_set_ipv4

Definition at line 252 of file up_down.py.

7.150.3.5 rpki.up_down.issue_pdu.req_resource_set_ipv6

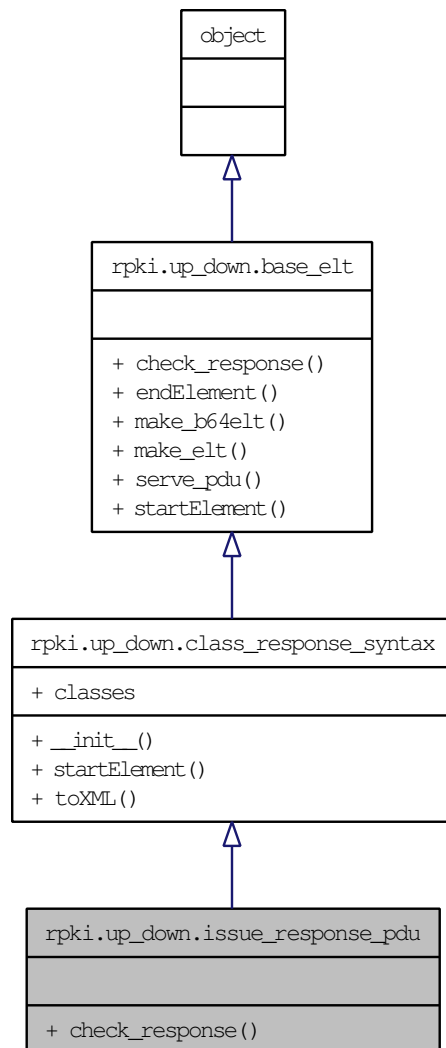
Definition at line 253 of file up_down.py.

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

- [up_down.py \(1873\)](#)

7.151 rpki.up_down.issue_response_pdu Class Reference

Inheritance diagram for rpki.up_down.issue_response_pdu:



Public Member Functions

- def [check_response](#)

7.151.1 Detailed Description

Up-Down protocol "issue_response" PDU.

Definition at line 335 of file up_down.py.

7.151.2 Member Function Documentation

7.151.2.1 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](#).

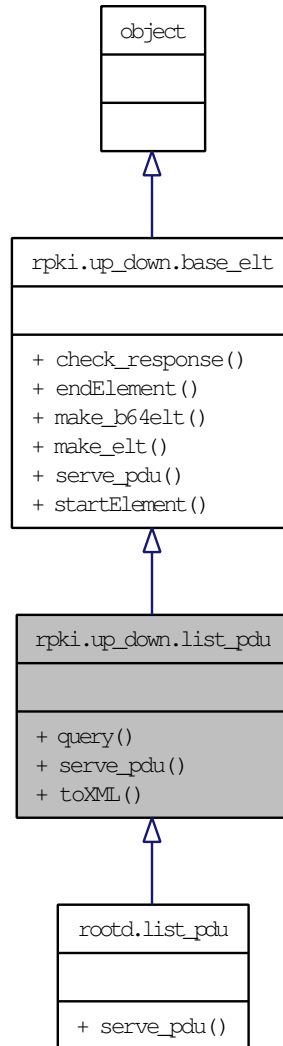
Definition at line 338 of file up_down.py.

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

- [up_down.py \(1873\)](#)

7.152 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](#)

7.152.1 Detailed Description

Up-Down protocol "list" PDU.

Definition at line 181 of file up_down.py.

7.152.2 Member Function Documentation

7.152.2.1 def rpki.up_down.list_pdu.query (*cls*, *parent*)

Send a "list" query to parent.

Definition at line 216 of file up_down.py.

7.152.2.2 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](#).

Reimplemented in [rootd.list_pdu](#).

Definition at line 188 of file up_down.py.

7.152.2.3 def rpki.up_down.list_pdu.toXML (*self*)

Generate (empty) payload of "list" PDU.

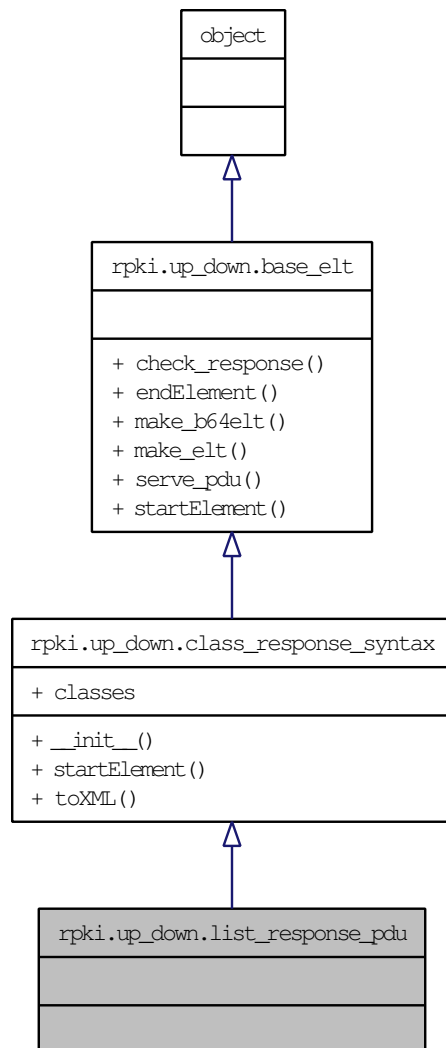
Definition at line 184 of file up_down.py.

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

- [up_down.py](#) (1873)

7.153 rpki.up_down.list_response_pdu Class Reference

Inheritance diagram for rpki.up_down.list_response_pdu:



7.153.1 Detailed Description

Up-Down protocol "list_response" PDU.

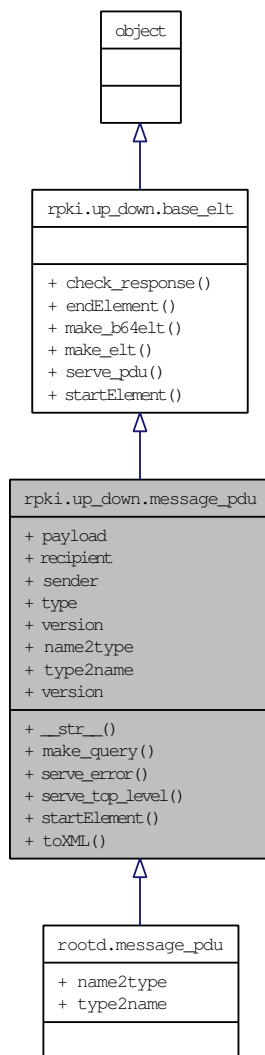
Definition at line 239 of file `up_down.py`.

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

- [up_down.py \(1873\)](#)

7.154 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

7.154.1 Detailed Description

Up-Down protocol message wrapper PDU.

Definition at line 447 of file up_down.py.

7.154.2 Member Function Documentation

7.154.2.1 def rpki.up_down.message_pdu.__str__ (self)

Convert a message PDU to a string.

Definition at line 484 of file up_down.py.

7.154.2.2 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.

7.154.2.3 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.

7.154.2.4 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.

7.154.2.5 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.

7.154.2.6 def rpki.up_down.message_pdu.toXML (self)

Generate payload of message PDU.

Definition at line 463 of file up_down.py.

7.154.3 Member Data Documentation

7.154.3.1 dictionary rpki.up_down.message_pdu.name2type [static]

Initial value:

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

Reimplemented in [rootd.message_pdu](#).

Definition at line 452 of file up_down.py.

7.154.3.2 `rpki.up_down.message_pdu.payload`

Definition at line 481 of file `up_down.py`.

7.154.3.3 `rpki.up_down.message_pdu.recipient`

Definition at line 479 of file `up_down.py`.

7.154.3.4 `rpki.up_down.message_pdu.sender`

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

7.154.3.5 `rpki.up_down.message_pdu.type`

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

7.154.3.6 `tuple rpki.up_down.message_pdu.type2name = dict((v,k) for k,v in name2type.items())` `[static]`

Reimplemented in [rootd.message_pdu](#).

Definition at line 461 of file `up_down.py`.

7.154.3.7 `rpki.up_down.message_pdu.version`

Definition at line 477 of file `up_down.py`.

7.154.3.8 `int rpki.up_down.message_pdu.version = 1` `[static]`

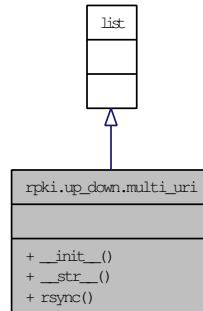
Definition at line 450 of file `up_down.py`.

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

- [up_down.py](#) (1873)

7.155 rpki.up_down.multi_uri Class Reference

Inheritance diagram for rpki.up_down.multi_uri:



Public Member Functions

- def [__init__](#)
- def [__str__](#)
- def [rsync](#)

7.155.1 Detailed Description

Container for a set of URIs.

Definition at line 73 of file up_down.py.

7.155.2 Member Function Documentation

7.155.2.1 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.

7.155.2.2 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.

7.155.2.3 def rpki.up_down.multi_uri.rsync (*self*)

Find first rsync://... URI in self.

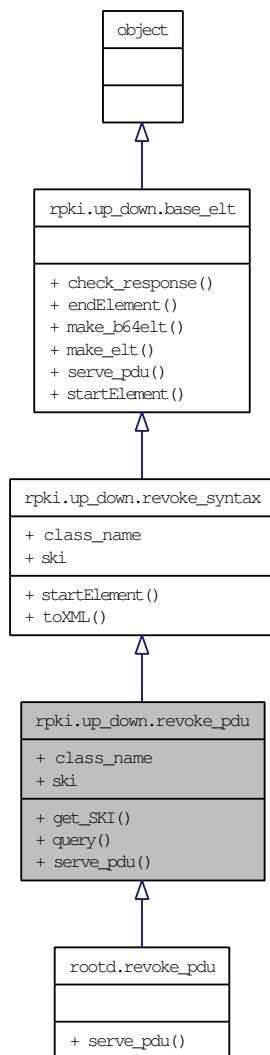
Definition at line 92 of file up_down.py.

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

- [up_down.py \(1873\)](#)

7.156 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](#)

7.156.1 Detailed Description

Up-Down protocol "revoke" PDU.

Definition at line 357 of file up_down.py.

7.156.2 Member Function Documentation

7.156.2.1 `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.

7.156.2.2 `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.

7.156.2.3 `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](#).

Reimplemented in [rootd.revoke_pdu](#).

Definition at line 364 of file up_down.py.

7.156.3 Member Data Documentation

7.156.3.1 `rpki.up_down.revoke_pdu.class_name`

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

Definition at line 380 of file up_down.py.

7.156.3.2 `rpki.up_down.revoke_pdu.ski`

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

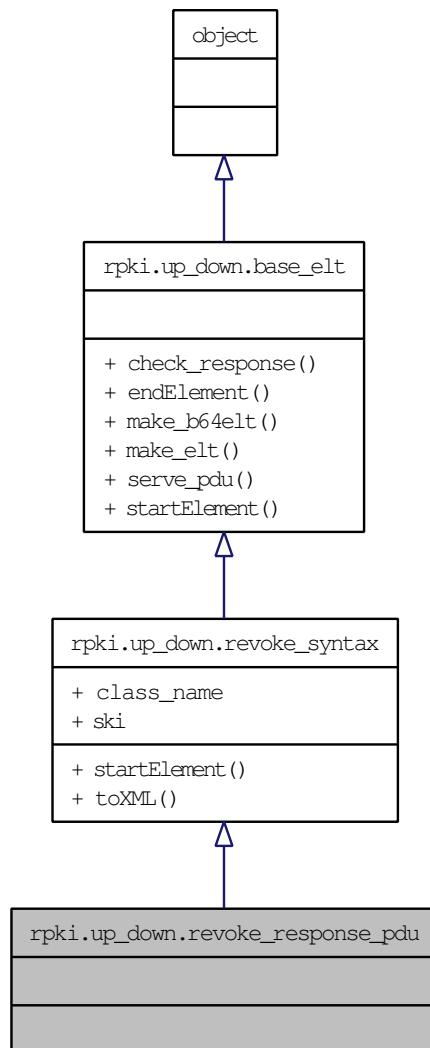
Definition at line 381 of file `up_down.py`.

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

- [up_down.py](#) (1873)

7.157 rpki.up_down.revoke_response_pdu Class Reference

Inheritance diagram for rpki.up_down.revoke_response_pdu:



7.157.1 Detailed Description

Up-Down protocol "revoke_response" PDU.

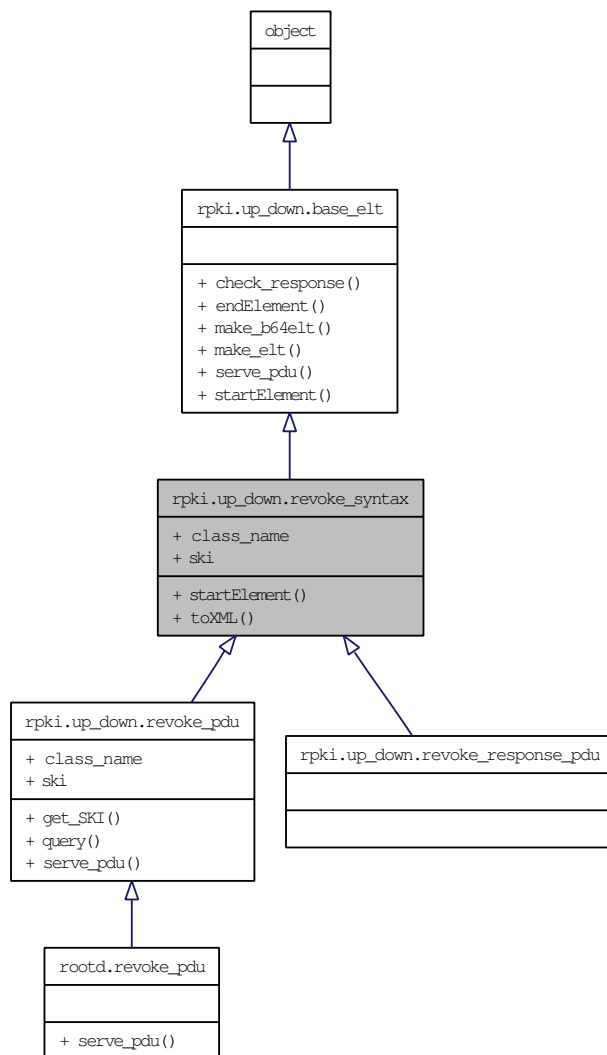
Definition at line 384 of file `up_down.py`.

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

- [up_down.py \(1873\)](#)

7.158 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](#)

7.158.1 Detailed Description

Syntax for Up-Down protocol "revoke" and "revoke_response" PDUs.

Definition at line 345 of file up_down.py.

7.158.2 Member Function Documentation

7.158.2.1 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.

7.158.2.2 def rpki.up_down.revoke_syntax.toXML (*self*)

Generate payload of "revoke" PDU.

Definition at line 353 of file up_down.py.

7.158.3 Member Data Documentation

7.158.3.1 rpki.up_down.revoke_syntax.class_name

Reimplemented in [rpki.up_down.revoke_pdu](#).

Definition at line 350 of file up_down.py.

7.158.3.2 `rpki.up_down.revoke_syntax.ski`

Reimplemented in [rpki.up_down.revoke_pdu](#).

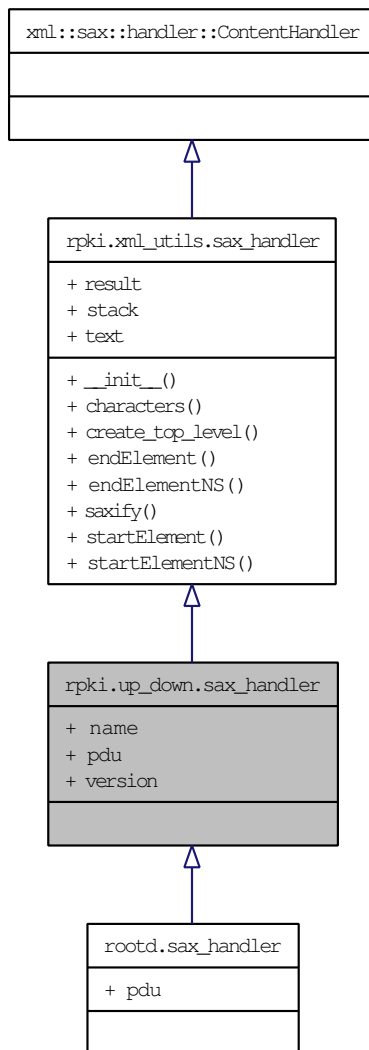
Definition at line 351 of file `up_down.py`.

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

- [up_down.py](#) (1873)

7.159 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"

7.159.1 Detailed Description

SAX handler for Up-Down protocol.

Definition at line 521 of file up_down.py.

7.159.2 Member Data Documentation

7.159.2.1 string rpki.up_down.sax_handler.name = "message" [static]

Definition at line 525 of file up_down.py.

7.159.2.2 rpki.up_down.sax_handler.pdu = message_pdu [static]

Reimplemented in [rootd.sax_handler](#).

Definition at line 524 of file up_down.py.

7.159.2.3 string rpki.up_down.sax_handler.version = "1" [static]

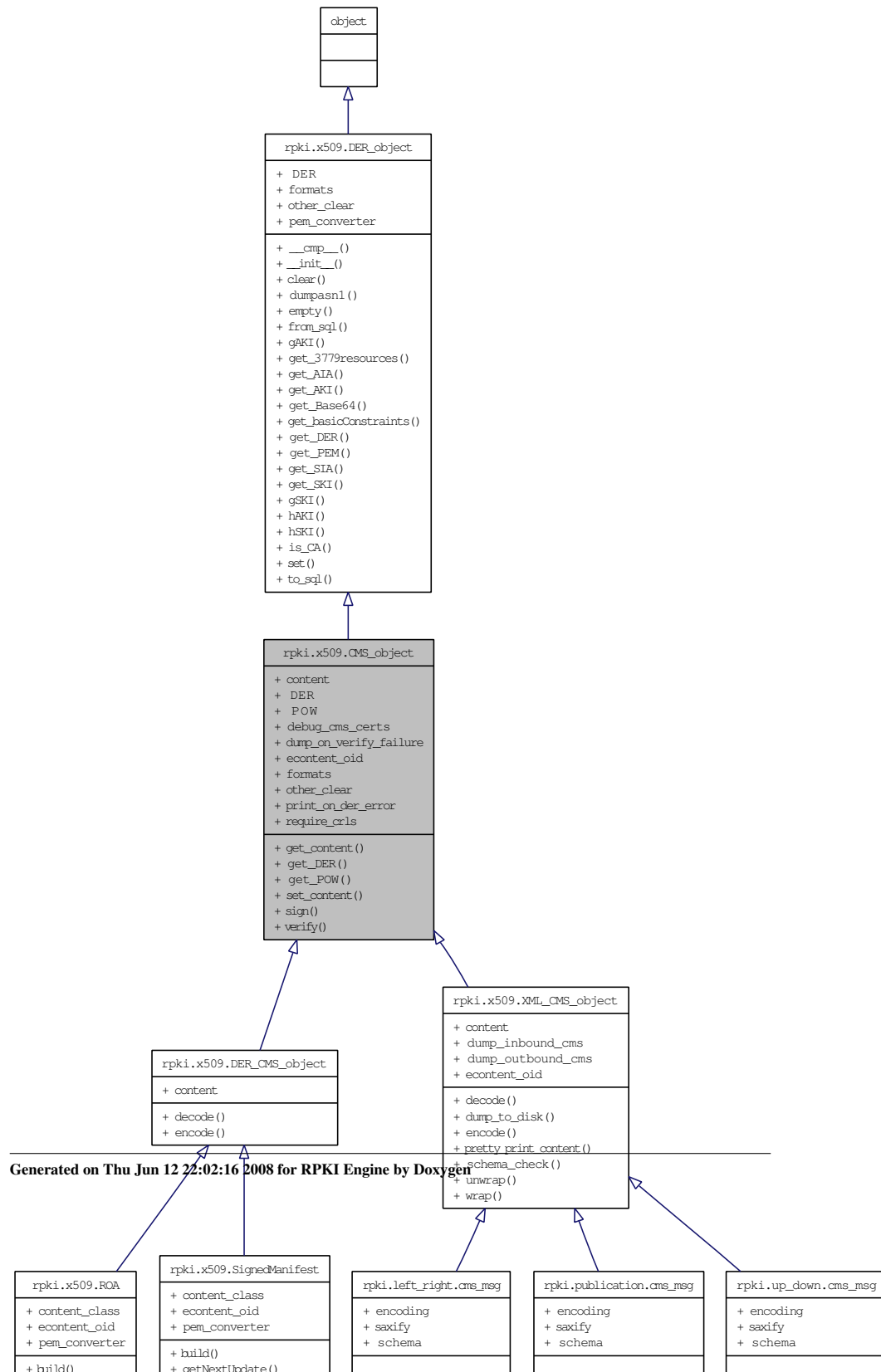
Definition at line 526 of file up_down.py.

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

- [up_down.py \(1873\)](#)

7.160 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.

7.160.1 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.

7.160.2 Member Function Documentation

7.160.2.1 def rpki.x509.CMS_object.get_content (self)

Get the inner content of this CMS_object.

Definition at line 639 of file x509.py.

7.160.2.2 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.

7.160.2.3 def rpki.x509.CMS_object.get_POW (self)

Get the POW value of this CMS_object.

Definition at line 632 of file x509.py.

7.160.2.4 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.

7.160.2.5 `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.

7.160.2.6 `def rpki.x509.CMS_object.verify (self, ta)`

Verify CMS wrapper and store inner content.

Definition at line 649 of file x509.py.

7.160.3 Member Data Documentation

7.160.3.1 `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.

7.160.3.2 `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.

7.160.3.3 `rpki.x509.CMS_object.DER`

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 628 of file x509.py.

7.160.3.4 `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.

7.160.3.5 `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.

7.160.3.6 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.

7.160.3.7 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.

7.160.3.8 rpki.x509.CMS_object.POW

Definition at line 636 of file x509.py.

7.160.3.9 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 traceback or something.

Definition at line 620 of file x509.py.

7.160.3.10 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 unconditionally mandatory in such cases.

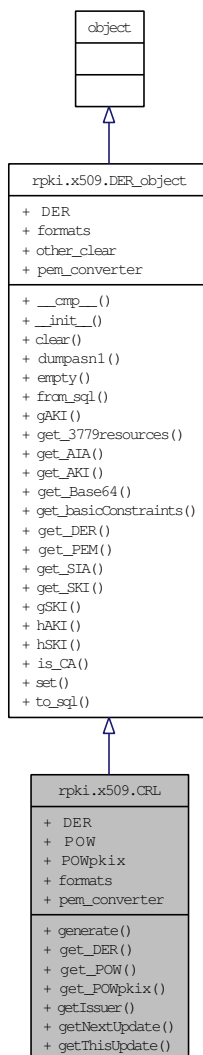
Definition at line 614 of file x509.py.

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

- [x509.py \(1873\)](#)

7.161 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](#).

7.161.1 Detailed Description

Class to hold a Certificate Revocation List.

Definition at line 889 of file x509.py.

7.161.2 Member Function Documentation

7.161.2.1 def [rpki.x509.CRL.generate](#) (*cls*, *keypair*, *issuer*, *serial*, *thisUpdate*, *nextUpdate*, *revokedCertificates*, *version* = 1, *digestType* = "sha256WithRSAEncryption")

Definition at line 937 of file x509.py.

7.161.2.2 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.

7.161.2.3 def rpki.x509.CRL.get_POW (*self*)

Get the POW value of this CRL.

Definition at line 908 of file x509.py.

7.161.2.4 def rpki.x509.CRL.get_POWpkix (*self*)

Get the POW.pkix value of this CRL.

Definition at line 915 of file x509.py.

7.161.2.5 def rpki.x509.CRL.getIssuer (*self*)

Get issuer value of this CRL.

Definition at line 932 of file x509.py.

7.161.2.6 def rpki.x509.CRL.getNextUpdate (*self*)

Get nextUpdate value from this CRL.

Definition at line 928 of file x509.py.

7.161.2.7 def rpki.x509.CRL.getThisUpdate (*self*)

Get thisUpdate value from this CRL.

Definition at line 924 of file x509.py.

7.161.3 Member Data Documentation**7.161.3.1 rpki.x509.CRL.DER**

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 901 of file x509.py.

7.161.3.2 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.

7.161.3.3 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.

7.161.3.4 rpki.x509.CRL.POW

Definition at line 912 of file x509.py.

7.161.3.5 rpki.x509.CRL.POWpkix

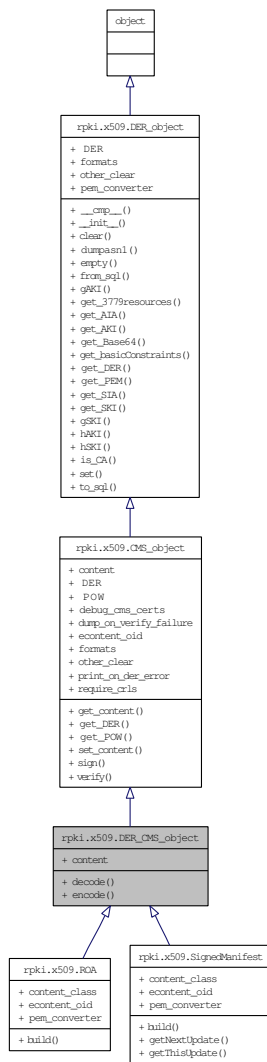
Definition at line 921 of file x509.py.

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

- [x509.py \(1873\)](#)

7.162 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](#)

7.162.1 Detailed Description

Class to hold CMS objects with DER-based content.

Definition at line 747 of file x509.py.

7.162.2 Member Function Documentation

7.162.2.1 `def rpki.x509.DER_CMS_object.decode (self, der)`

Decode DER and set inner content.

Definition at line 754 of file x509.py.

7.162.2.2 `def rpki.x509.DER_CMS_object.encode (self)`

Encode inner content for signing.

Definition at line 750 of file x509.py.

7.162.3 Member Data Documentation

7.162.3.1 `rpki.x509.DER_CMS_object.content`

Reimplemented from [rpki.x509.CMS_object](#).

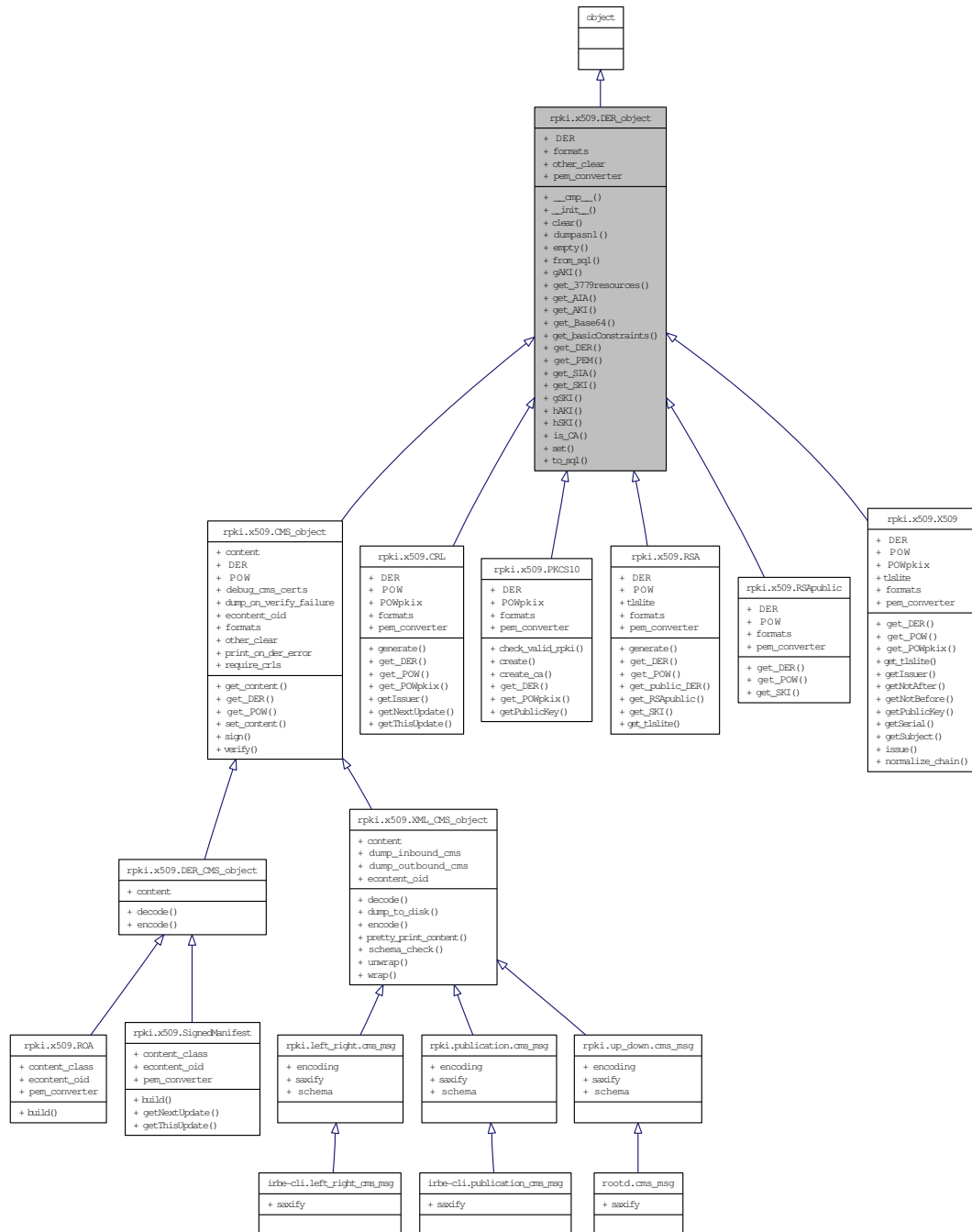
Definition at line 758 of file x509.py.

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

- [x509.py \(1873\)](#)

7.163 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](#).

7.163.1 Detailed Description

Virtual class to hold a generic DER object.

Definition at line 76 of file x509.py.

7.163.2 Member Function Documentation

7.163.2.1 `def rpki.x509.DER_object.__cmp__ (self, other)`

Compare two DER-encoded objects.

Definition at line 160 of file x509.py.

7.163.2.2 `def rpki.x509.DER_object.__init__ (self, kw)`

Initialize a DER_object.

Definition at line 103 of file x509.py.

7.163.2.3 `def rpki.x509.DER_object.clear (self)`

Make this object empty.

Definition at line 98 of file x509.py.

7.163.2.4 `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.

7.163.2.5 `def rpki.x509.DER_object.empty (self)`

Test whether this object is empty.

Definition at line 91 of file x509.py.

7.163.2.6 def rpki.x509.DER_object.from_sql (cls, x)

Convert from SQL storage format.

Definition at line 228 of file x509.py.

7.163.2.7 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.

7.163.2.8 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.

7.163.2.9 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.

7.163.2.10 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.

7.163.2.11 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.

7.163.2.12 def rpki.x509.DER_object.get_basicConstraints (self)

Get the basicConstraints extension from this object. Only works for subclasses that support getExtension().

Definition at line 207 of file x509.py.

7.163.2.13 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.

7.163.2.14 def rpki.x509.DER_object.get_PEM (self)

Get the PEM representation of this object.

Definition at line 156 of file x509.py.

7.163.2.15 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.

7.163.2.16 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.

7.163.2.17 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.

7.163.2.18 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.

7.163.2.19 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.

7.163.2.20 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.

7.163.2.21 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.

7.163.2.22 def rpki.x509.DER_object.to_sql (self)

Convert to SQL storage format.

Definition at line 232 of file x509.py.

7.163.3 Member Data Documentation**7.163.3.1 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.

7.163.3.2 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.

7.163.3.3 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.

7.163.3.4 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](#).

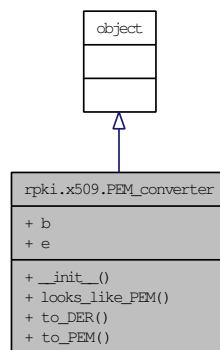
Definition at line 83 of file x509.py.

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

- [x509.py \(1873\)](#)

7.164 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](#)

7.164.1 Detailed Description

Convert between DER and PEM encodings for various kinds of ASN.1 data.

Definition at line 43 of file x509.py.

7.164.2 Member Function Documentation

7.164.2.1 `def rpki.x509.PEM_converter.__init__ (self, kind)`

Initialize PEM_converter.

Definition at line 46 of file x509.py.

7.164.2.2 `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.

7.164.2.3 `def rpki.x509.PEM_converter.to_DER (self, pem)`

Convert from PEM to DER.

Definition at line 56 of file x509.py.

7.164.2.4 `def rpki.x509.PEM_converter.to_PEM (self, der)`

Convert from DER to PEM.

Definition at line 67 of file x509.py.

7.164.3 Member Data Documentation

7.164.3.1 rpki.x509.PEM_converter.b

Definition at line 48 of file x509.py.

7.164.3.2 rpki.x509.PEM_converter.e

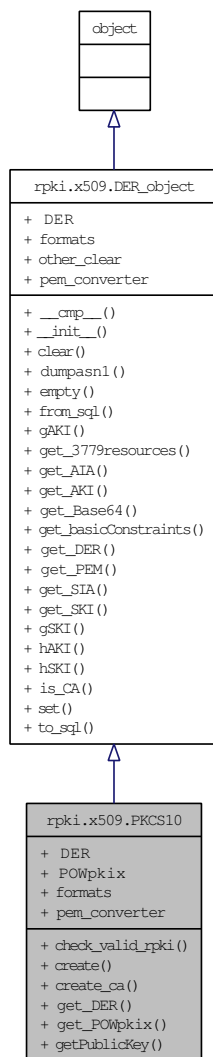
Definition at line 49 of file x509.py.

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

- [x509.py \(1873\)](#)

7.165 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](#).

7.165.1 Detailed Description

Class to hold a PKCS #10 request.

Definition at line 402 of file x509.py.

7.165.2 Member Function Documentation

7.165.2.1 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.

7.165.2.2 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.

7.165.2.3 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.

7.165.2.4 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.

7.165.2.5 def rpki.x509.PKCS10.get_POWpkix (self)

Get the POW.pkix value of this certification request.

Definition at line 418 of file x509.py.

7.165.2.6 def rpki.x509.PKCS10.getPublicKey (self)

Extract the public key from this certification request.

Definition at line 427 of file x509.py.

7.165.3 Member Data Documentation**7.165.3.1 rpki.x509.PKCS10.DER**

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 414 of file x509.py.

**7.165.3.2 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.

7.165.3.3 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.

7.165.3.4 rpki.x509.PKCS10.POWpkix

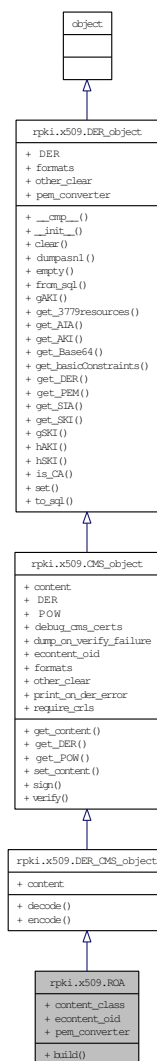
Definition at line 424 of file x509.py.

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

- [x509.py \(1873\)](#)

7.166 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](#).

7.166.1 Detailed Description

Class to hold a signed ROA.

Definition at line 796 of file x509.py.

7.166.2 Member Function Documentation

7.166.2.1 `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.

7.166.3 Member Data Documentation

7.166.3.1 `rpki.x509.ROA.content_class = rpki.roa.RouteOriginAttestation`
[static]

Definition at line 800 of file x509.py.

7.166.3.2 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.

7.166.3.3 tuple `rpki.x509.ROA.pem_converter = PEM_converter("ROUTE ORIGIN ATTESTATION")` [static]

PEM converter for this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

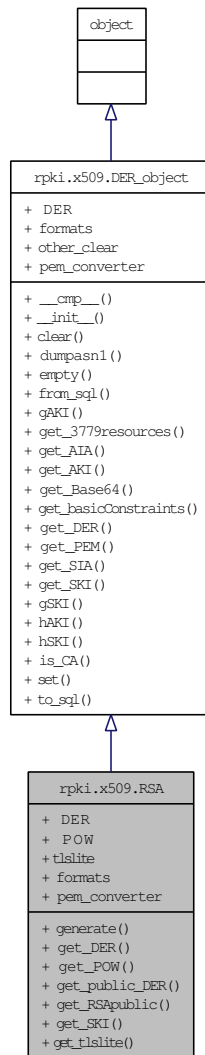
Definition at line 799 of file x509.py.

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

- [x509.py \(1873\)](#)

7.167 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_tslite](#)

Public Attributes

- [DER](#)
DER value of this [object](#).
- [POW](#)
- [tslite](#)

Static Public Attributes

- tuple [formats](#) = ("DER", "POW", "tslite")
Formats supported in this [object](#).
- tuple [pem_converter](#) = [PEM_converter](#)("RSA PRIVATE KEY")
PEM converter for this [object](#).

7.167.1 Detailed Description

Class to hold an RSA key pair.

Definition at line 500 of file x509.py.

7.167.2 Member Function Documentation

7.167.2.1 def rpki.x509.RSA.generate (*self*, *keylength* = 2048)

Generate a new keypair.

Definition at line 530 of file x509.py.

7.167.2.2 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.

7.167.2.3 def rpki.x509.RSA.get_POW (self)

Get the POW value of this keypair.

Definition at line 516 of file x509.py.

7.167.2.4 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.

7.167.2.5 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.

7.167.2.6 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.

7.167.2.7 def rpki.x509.RSA.get_tlslite (self)

Get the tlslite value of this keypair.

Definition at line 523 of file x509.py.

7.167.3 Member Data Documentation

7.167.3.1 rpki.x509.RSA.DER

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 512 of file x509.py.

7.167.3.2 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.

7.167.3.3 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.

7.167.3.4 rpki.x509.RSA.POW

Definition at line 520 of file x509.py.

7.167.3.5 rpki.x509.RSA.tlslite

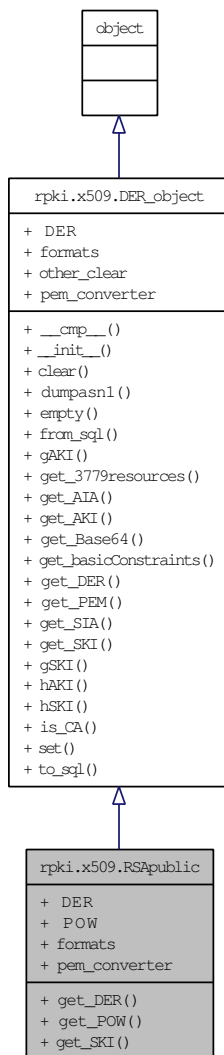
Definition at line 527 of file x509.py.

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

- [x509.py \(1873\)](#)

7.168 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](#).

7.168.1 Detailed Description

Class to hold an RSA public key.

Definition at line 547 of file x509.py.

7.168.2 Member Function Documentation

7.168.2.1 `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.

7.168.2.2 `def rpki.x509.RSAPublic.get_POW (self)`

Get the POW value of this public key.

Definition at line 563 of file x509.py.

7.168.2.3 `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.

7.168.3 Member Data Documentation

7.168.3.1 rpki.x509.RSAPublic.DER

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 559 of file x509.py.

7.168.3.2 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.

7.168.3.3 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.

7.168.3.4 rpki.x509.RSAPublic.POW

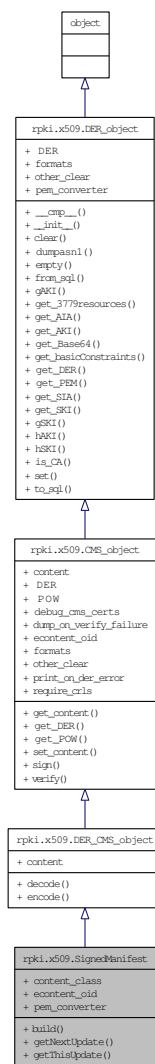
Definition at line 567 of file x509.py.

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

- [x509.py \(1873\)](#)

7.169 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](#).

7.169.1 Detailed Description

Class to hold a signed manifest.

Definition at line 760 of file x509.py.

7.169.2 Member Function Documentation

7.169.2.1 `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.

7.169.2.2 `def rpki.x509.SignedManifest.getNextUpdate (self)`

Get nextUpdate value from this manifest.

Definition at line 771 of file x509.py.

7.169.2.3 `def rpki.x509.SignedManifest.getThisUpdate (self)`

Get thisUpdate value from this manifest.

Definition at line 767 of file x509.py.

7.169.3 Member Data Documentation

7.169.3.1 `rpki.x509.SignedManifest.content_class` = `rpki.manifest.Manifest`
[static]

Definition at line 764 of file x509.py.

7.169.3.2 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.

7.169.3.3 tuple rpki.x509.SignedManifest.pem_converter = PEM_converter("RPKI MANIFEST") `[static]`

PEM converter for this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

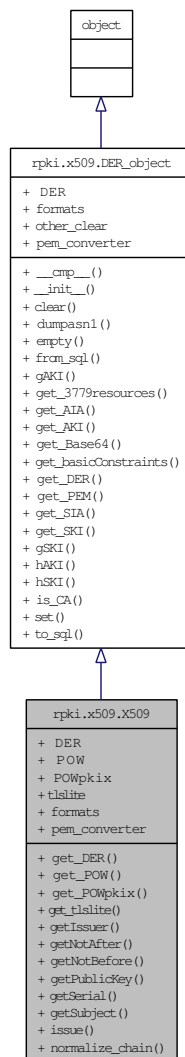
Definition at line 763 of file x509.py.

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

- [x509.py \(1873\)](#)

7.170 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_tlsite](#)

- 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](#)
- [tsslite](#)

Static Public Attributes

- tuple [formats](#) = ("DER", "POW", "POWpkix", "tsslite")
Formats supported in this [object](#).
- tuple [pem_converter](#) = [PEM_converter](#)("CERTIFICATE")
PEM converter for this [object](#).

7.170.1 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.

7.170.2 Member Function Documentation

7.170.2.1 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.

7.170.2.2 def rpki.x509.X509.get_POW (*self*)

Get the POW value of this certificate.

Definition at line 287 of file x509.py.

7.170.2.3 def rpki.x509.X509.get_POWpkix (*self*)

Get the POW.pkix value of this certificate.

Definition at line 294 of file x509.py.

7.170.2.4 def rpki.x509.X509.get_tlslite (*self*)

Get the tlslite value of this certificate.

Definition at line 303 of file x509.py.

7.170.2.5 def rpki.x509.X509.getIssuer (*self*)

Get the issuer of this certificate.

Definition at line 312 of file x509.py.

7.170.2.6 def rpki.x509.X509.getNotAfter (*self*)

Get the expiration time of this certificate.

Definition at line 324 of file x509.py.

7.170.2.7 def rpki.x509.X509.getNotBefore (*self*)

Get the inception time of this certificate.

Definition at line 320 of file x509.py.

7.170.2.8 def rpki.x509.X509.getPublicKey (self)

Extract the public key from this certificate.

Definition at line 332 of file x509.py.

7.170.2.9 def rpki.x509.X509.getSerial (self)

Get the serial number of this certificate.

Definition at line 328 of file x509.py.

7.170.2.10 def rpki.x509.X509.getSubject (self)

Get the subject of this certificate.

Definition at line 316 of file x509.py.

7.170.2.11 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.

7.170.2.12 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.

7.170.3 Member Data Documentation**7.170.3.1 rpki.x509.X509.DER**

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 274 of file x509.py.

7.170.3.2 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.

7.170.3.3 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.

7.170.3.4 rpki.x509.X509.POW

Definition at line 291 of file x509.py.

7.170.3.5 rpki.x509.X509.POWpkix

Definition at line 300 of file x509.py.

7.170.3.6 rpki.x509.X509.tlslite

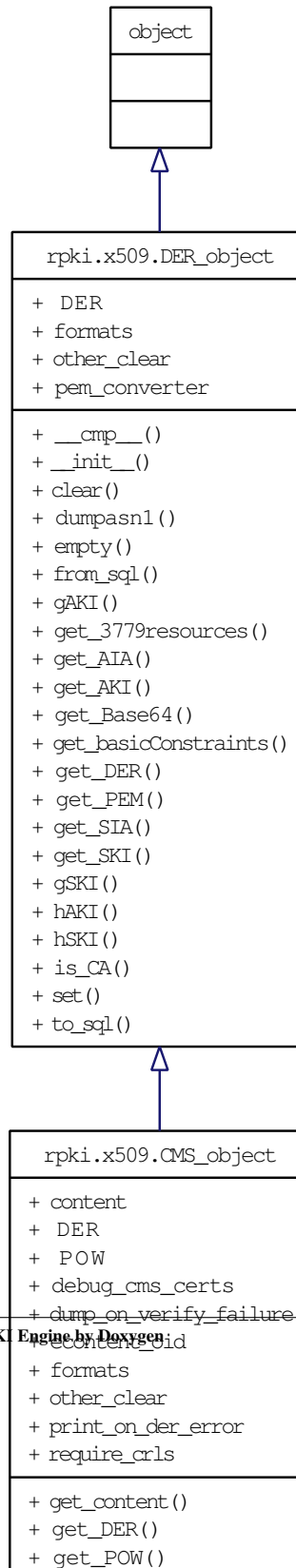
Definition at line 309 of file x509.py.

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

- [x509.py \(1873\)](#)

7.171 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")

7.171.1 Detailed Description

Class to hold CMS-wrapped XML protocol data.

Definition at line 815 of file x509.py.

7.171.2 Member Function Documentation

7.171.2.1 def rpki.x509.XML_CMS_object.decode (*self*, *xml*)

Decode XML and set inner content.

Definition at line 838 of file x509.py.

7.171.2.2 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.

7.171.2.3 def rpki.x509.XML_CMS_object.encode (*self*)

Encode inner content for signing.

Definition at line 834 of file x509.py.

7.171.2.4 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.

7.171.2.5 def rpki.x509.XML_CMS_object.schema_check (*self*)

Handle XML RelaxNG schema check.

Definition at line 846 of file x509.py.

7.171.2.6 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.

7.171.2.7 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.

7.171.3 Member Data Documentation

7.171.3.1 rpki.x509.XML_CMS_object.content

Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 840 of file x509.py.

7.171.3.2 rpki.x509.XML_CMS_object.dump_inbound_cms = None
[static]

Definition at line 832 of file x509.py.

7.171.3.3 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.

7.171.3.4 tuple rpki.x509.XML_CMS_object.econtent_oid = POWify_OID("id-ct-xml") [static]

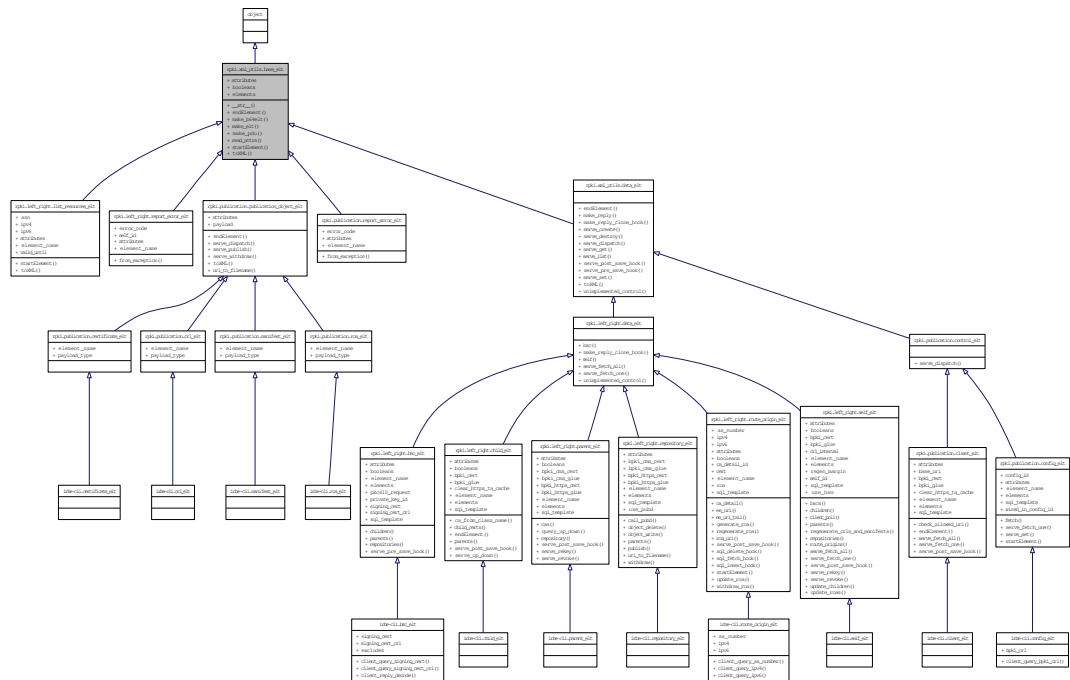
Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 818 of file x509.py.

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

- [x509.py \(1873\)](#)

Inheritance diagram for `rpki.xml_utils.base_elt`:



- def `__str__`
- def `endElement`
- def `make_b64elt`
- def `make_elt`
- def `make_pdu`
- def `read_attrs`
- def `startElement`
- def `toXML`

- 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.

7.172.1 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`.

7.172.2 Member Function Documentation

7.172.2.1 `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`.

7.172.2.2 `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`.

7.172.2.3 `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`.

7.172.2.4 `def rpki.xml_utils.base_elt.make_elt (self)`

XML element constructor.

Definition at line 144 of file `xml_utils.py`.

7.172.2.5 def rpki.xml_utils.base_elt.make_pdu (cls, kargs)

Generic PDU constructor.

Definition at line 168 of file xml_utils.py.

7.172.2.6 def rpki.xml_utils.base_elt.read_attrs (self, attrs)

Template-driven attribute reader.

Definition at line 134 of file xml_utils.py.

7.172.2.7 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.

7.172.2.8 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.

7.172.3 Member Data Documentation

7.172.3.1 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.

7.172.3.2 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`.

7.172.3.3 rpki::xml_utils.base_elt::elements = () [static]

XML elements contained by this element.

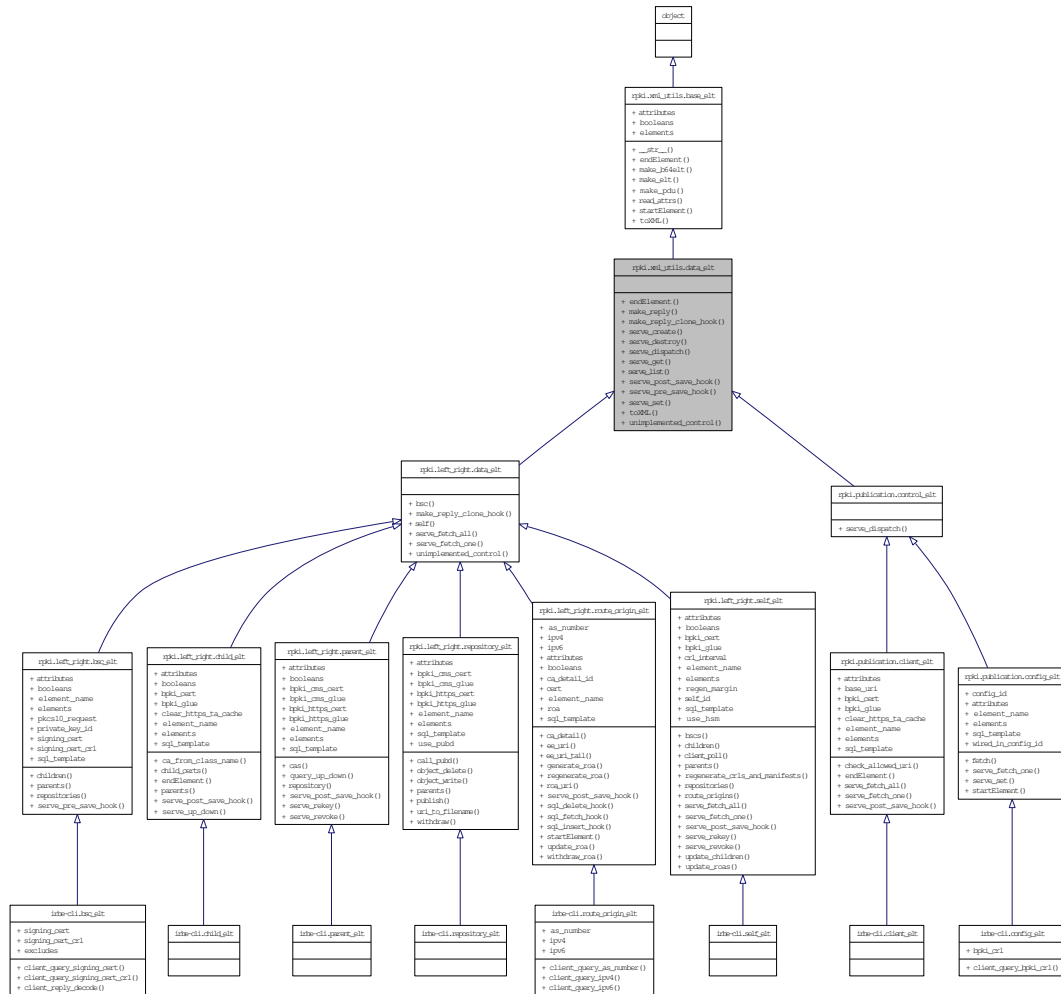
Reimplemented in [rpki.left_right.self_elt](#), [rpki.left_right.bsc_elt](#), [rpki.left_right.parent_elt](#), [rpki.left_right.child_elt](#), [rpki.left_right.repository_elt](#), [rpki.publication.config_elt](#), and [rpki.publication.client_elt](#).

Definition at line 113 of file `xml_utils.py`.

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

- [xml_utils.py \(1873\)](#)

Inheritance diagram for `rpki.xml_utils.data_elt`:



- 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](#)

7.173.1 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`.

7.173.2 Member Function Documentation

7.173.2.1 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`.

7.173.2.2 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`.

7.173.2.3 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`.

7.173.2.4 def rpki.xml_utils.data_elt.serve_create (self, r_msg)

Handle a create action.

Definition at line 231 of file xml_utils.py.

7.173.2.5 def rpki.xml_utils.data_elt.serve_destroy (self, r_msg)

Handle a destroy action.

Definition at line 266 of file xml_utils.py.

7.173.2.6 def rpki.xml_utils.data_elt.serve_dispatch (self, r_msg)

Action dispatch handler.

Definition at line 272 of file xml_utils.py.

7.173.2.7 def rpki.xml_utils.data_elt.serve_get (self, r_msg)

Handle a get action.

Definition at line 254 of file xml_utils.py.

7.173.2.8 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.

7.173.2.9 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.

7.173.2.10 `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.

7.173.2.11 `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.

7.173.2.12 `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.

7.173.2.13 `def rpki.xml_utils.data_elt.unimplemented_control (self, controls)`

Uniform handling for unimplemented control operations.

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

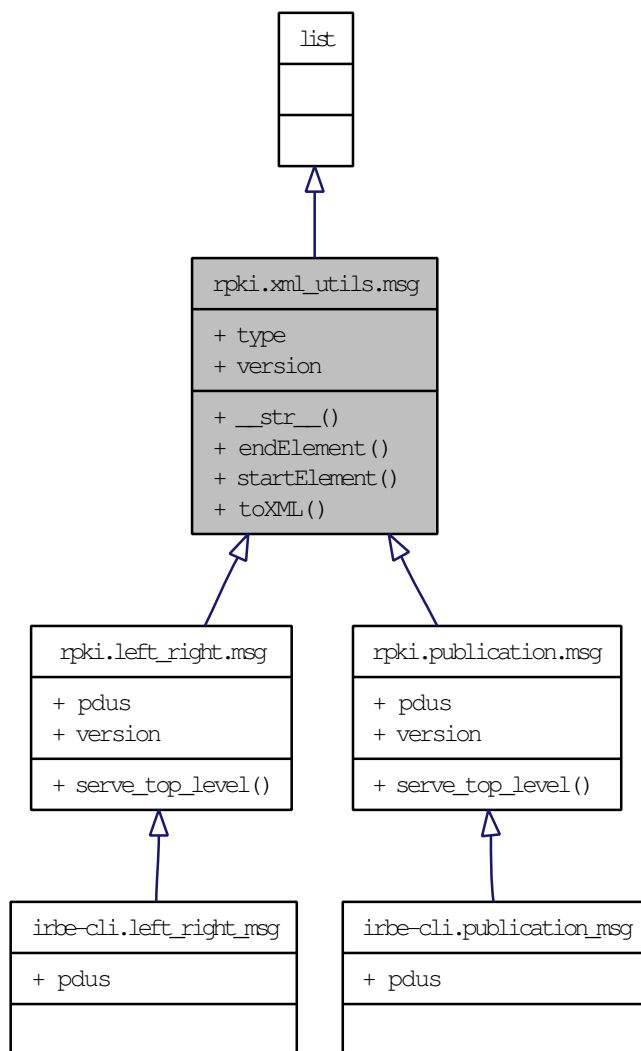
Definition at line 283 of file xml_utils.py.

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

- [xml_utils.py](#) (1873)

7.174 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](#)

7.174.1 Detailed Description

Generic top-level PDU.

Definition at line 289 of file xml_utils.py.

7.174.2 Member Function Documentation

7.174.2.1 `def rpki.xml_utils.msg.__str__ (self)`

Convert msg object to string.

Definition at line 309 of file xml_utils.py.

7.174.2.2 `def rpki.xml_utils.msg.endElement (self, stack, name, text)`

Handle top-level PDU.

Definition at line 303 of file xml_utils.py.

7.174.2.3 `def rpki.xml_utils.msg.startElement (self, stack, name, attrs)`

Handle top-level PDU.

Definition at line 292 of file xml_utils.py.

7.174.2.4 `def rpki.xml_utils.msg.toXML (self)`

Generate top-level PDU.

Definition at line 313 of file xml_utils.py.

7.174.3 Member Data Documentation

7.174.3.1 `rpki.xml_utils.msg.type`

Definition at line 296 of file xml_utils.py.

7.174.3.2 rpki.xml_utils.msg.version

Reimplemented in [rpki.left_right.msg](#), and [rpki.publication.msg](#).

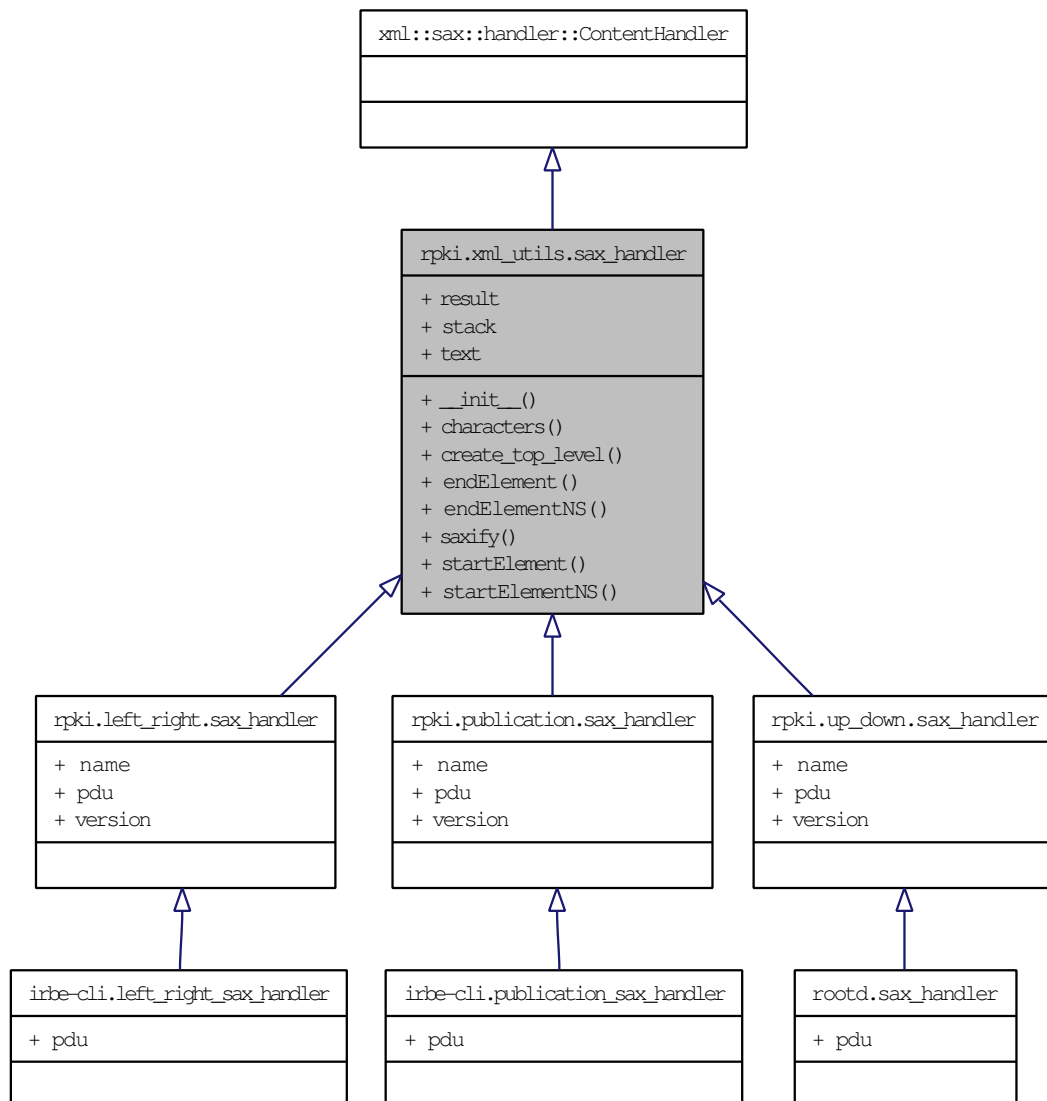
Definition at line 295 of file xml_utils.py.

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

- [xml_utils.py \(1873\)](#)

7.175 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](#)

7.175.1 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`.

7.175.2 Member Function Documentation

7.175.2.1 `def rpki.xml_utils.sax_handler.__init__ (self)`

Initialize SAX handler.

Definition at line 36 of file `xml_utils.py`.

7.175.2.2 `def rpki.xml_utils.sax_handler.characters (self, content)`

Accumulate a chunk of element content (text).

Definition at line 49 of file `xml_utils.py`.

7.175.2.3 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.

7.175.2.4 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.

7.175.2.5 def rpki.xml_utils.sax_handler.endElementNS (self, name, qname)

Redirect endElementNS() events to endElement().

Definition at line 45 of file xml_utils.py.

7.175.2.6 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.

7.175.2.7 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.

7.175.2.8 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.

7.175.3 Member Data Documentation

7.175.3.1 rpki.xml_utils.sax_handler.result

Definition at line 75 of file xml_utils.py.

7.175.3.2 rpki.xml_utils.sax_handler.stack

Definition at line 39 of file xml_utils.py.

7.175.3.3 rpki.xml_utils.sax_handler.text

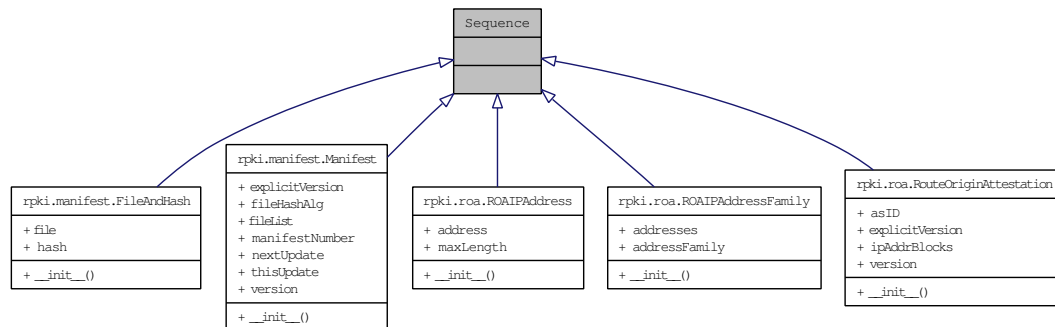
Definition at line 38 of file xml_utils.py.

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

- [xml_utils.py \(1873\)](#)

7.176 Sequence Class Reference

Inheritance diagram for Sequence:

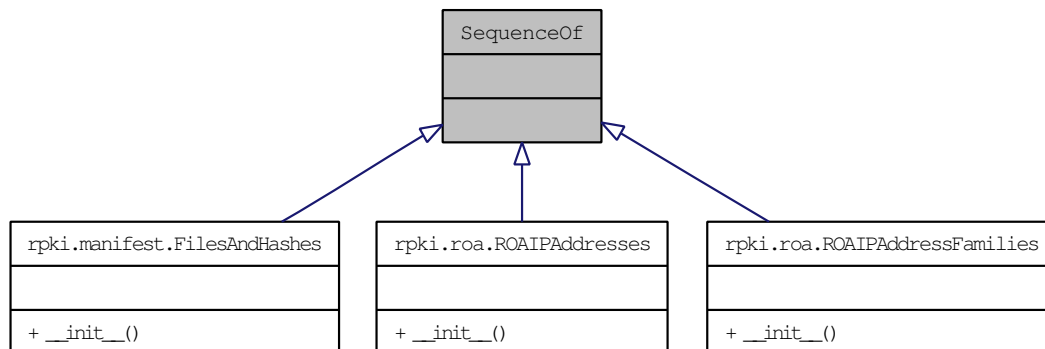


The documentation for this class was generated from the following file:

- [roa.py \(1873\)](#)

7.177 SequenceOf Class Reference

Inheritance diagram for SequenceOf:

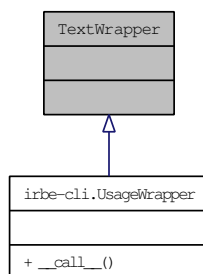


The documentation for this class was generated from the following file:

- [roa.py \(1873\)](#)

7.178 TextWrapper Class Reference

Inheritance diagram for TextWrapper:

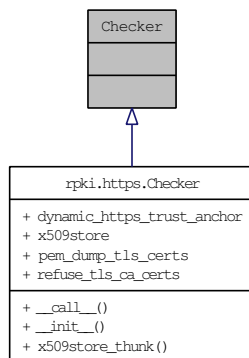


The documentation for this class was generated from the following file:

- [irbe-cli.py \(1880\)](#)

7.179 Checker Class Reference

Inheritance diagram for Checker:

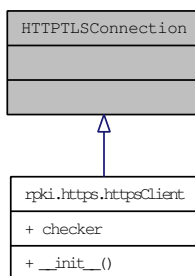


The documentation for this class was generated from the following file:

- [https.py \(1873\)](#)

7.180 HTTPTLSConnection Class Reference

Inheritance diagram for HTTPTLSConnection:

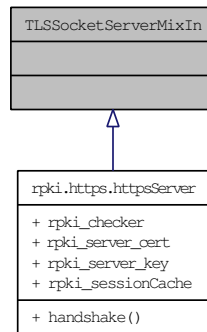


The documentation for this class was generated from the following file:

- [https.py \(1873\)](#)

7.181 TLSSocketServerMixIn Class Reference

Inheritance diagram for TLSSocketServerMixIn:

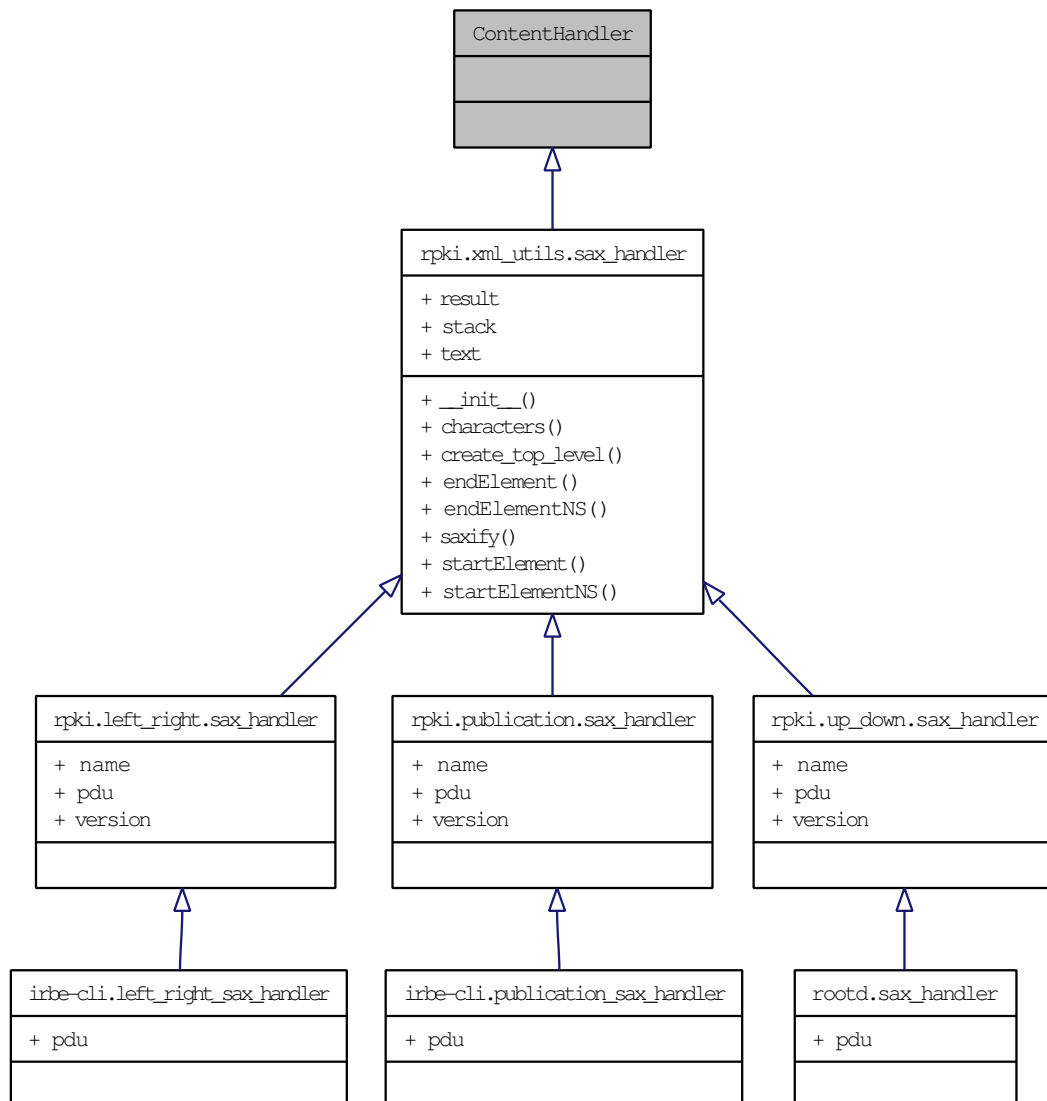


The documentation for this class was generated from the following file:

- [https.py \(1873\)](#)

7.182 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 `cross-certify.py` File Reference

Namespaces

- namespace [cross](#)
- namespace [cross-certify](#)

Functions

- def [cross-certify.usage](#)

Variables

- tuple [cross-certify.cert](#) = [rpki.x509.X509](#)(POWpkix = x)
- tuple [cross-certify.child](#) = [rpki.x509.X509](#)(Auto_file = a)
- tuple [cross-certify.f](#) = [open](#)(serial_file, "r")
- tuple [cross-certify.keypair](#) = [rpki.x509.RSA](#)(Auto_file = a)
- tuple [cross-certify.lifetime](#) = [rpki.sundial.timedelta](#)(days = 30)
- [cross-certify.notAfter](#) = now+lifetime
- tuple [cross-certify.now](#) = [rpki.sundial.now](#)()
- [cross-certify.output](#) = None
- tuple [cross-certify.parent](#) = [rpki.x509.X509](#)(Auto_file = a)
- tuple [cross-certify.serial](#) = f.read()

- `cross-certify.serial_file = a`
- tuple `cross-certify.x = POW.pkix.Certificate()`

8.4 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.DBConsistencyError`
- 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.UnexpectedCMSURLs](#)
- class [rpki.exceptions.UnparsableCMSDER](#)
- class [rpki.exceptions.UpstreamError](#)
- class [rpki.exceptions.WrongContentType](#)

8.5 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.tlsite_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"

8.6 ipaddrs.py File Reference

Namespaces

- namespace [rpki.ipaddrs](#)

Classes

- class [rpki.ipaddrs.v4addr](#)
- class [rpki.ipaddrs.v6addr](#)

8.7 irbe-cli.py File Reference

Namespaces

- namespace [irbe](#)
- namespace [irbe-cli](#)

Classes

- class [irbe-cli.bsc_elt](#)
- class [irbe-cli.certificate_elt](#)
- class [irbe-cli.child_elt](#)
- class [irbe-cli.client_elt](#)
- class [irbe-cli.cmd_elt_mixin](#)
- class [irbe-cli.cmd_msg_mixin](#)
- class [irbe-cli.config_elt](#)
- class [irbe-cli.crl_elt](#)
- class [irbe-cli.left_right_cms_msg](#)
- class [irbe-cli.left_right_msg](#)
- class [irbe-cli.left_right_sax_handler](#)
- class [irbe-cli.manifest_elt](#)
- class [irbe-cli.parent_elt](#)
- class [irbe-cli.publication_cms_msg](#)
- class [irbe-cli.publication_msg](#)
- class [irbe-cli.publication_sax_handler](#)
- class [irbe-cli.repository_elt](#)
- class [irbe-cli.roa_elt](#)
- class [irbe-cli.route_origin_elt](#)
- class [irbe-cli.self_elt](#)
- class [irbe-cli.UsageWrapper](#)

Functions

- def [irbe-cli.call_daemon](#)
- def [irbe-cli.usage](#)

Variables

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

8.8 irdbd.py File Reference

Namespaces

- namespace `irdbd`

Functions

- def `irdbd.handler`

Variables

- tuple `irdbd.bpki_ta` = `rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))`
- tuple `irdbd.cfg` = `rpki.config.parser(cfg_file, "irdbd")`
- string `irdbd.cfg_file` = `"irdbd.conf"`
- tuple `irdbd.client_ta` = `(bpki_ta, rpki_cert)`
- tuple `irdbd.cur` = `db.cursor()`
- tuple `irdbd.db`
- tuple `irdbd.handlers` = `((u.path, handler),)`
- string `irdbd.host` = `"localhost"`
- tuple `irdbd.irdbd_cert` = `rpki.x509.X509(Auto_file = cfg.get("irdbd-cert"))`

- tuple `irdbd.irdbd_key` = `rpki.x509.RSA`(`Auto_file` = `cfg.get("irdbd-key")`)
- int `irdbd.port` = 443
- tuple `irdbd.rpkid_cert` = `rpki.x509.X509`(`Auto_file` = `cfg.get("rpkid-cert")`)
- `irdbd.server_cert` = `irdbd_cert`,
- tuple `irdbd.startup_msg` = `cfg.get("startup-message", "")`
- tuple `irdbd.u` = `urlparse.urlparse(cfg.get("https-url"))`

8.9 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

8.10 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)`

8.11 manifest.py File Reference

Namespaces

- namespace `rpki.manifest`

Classes

- class `rpki.manifest.FileAndHash`
- class `rpki.manifest.FilesAndHashes`
- class `rpki.manifest.Manifest`

8.12 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.

8.13 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

8.14 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.

8.15 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.

8.16 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.

8.17 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](#)

8.18 rootd.py File Reference

Namespaces

- namespace [rootd](#)

Classes

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

Functions

- def [rootd.compose_response](#)
- def [rootd.del_subject_cert](#)
- def [rootd.get_subject_cert](#)
- def [rootd.set_subject_cert](#)
- def [rootd.stash_subject_pkcs10](#)
- def [rootd.up_down_handler](#)

Variables

- tuple [rootd.bpki_ta](#) = [rpki.x509.X509](#)(Auto_file = [cfg.get](#)("bpki-ta"))
- tuple [rootd.cfg](#) = [rpki.config.parser](#)([cfg_file](#), "rootd")
- string [rootd.cfg_file](#) = "rootd.conf"
- tuple [rootd.child_bpki_cert](#) = [rpki.x509.X509](#)(Auto_file = [cfg.get](#)("child-bpki-cert"))
- tuple [rootd.client_ta](#) = (bpki_ta, child_bpki_cert)
- [rootd.handlers](#) = up_down_handler)
- [rootd.host](#) = https_server_host,
- tuple [rootd.https_server_host](#) = [cfg.get](#)("server-host", "")
- tuple [rootd.https_server_port](#) = [int](#)([cfg.get](#)("server-port"))
- [rootd.port](#) = https_server_port,
- tuple [rootd.rootd_base](#) = [cfg.get](#)("rootd_base", "rsync://" + rootd_name + ".invalid/")
- tuple [rootd.rootd_bpki_cert](#) = [rpki.x509.X509](#)(Auto_file = [cfg.get](#)("rootd-bpki-cert"))
- tuple [rootd.rootd_bpki_crl](#) = [rpki.x509.CRL](#)(Auto_file = [cfg.get](#)("rootd-bpki-crl"))
- tuple [rootd.rootd_bpki_key](#) = [rpki.x509.RSA](#)(Auto_file = [cfg.get](#)("rootd-bpki-key"))
- tuple [rootd.rootd_cert](#) = [cfg.get](#)("rootd_cert", rootd_base + "rootd.cer")
- tuple [rootd.rootd_name](#) = [cfg.get](#)("rootd_name", "wombat")
- tuple [rootd.rpki_issuer](#) = [rpki.x509.X509](#)(Auto_file = [cfg.get](#)("rpki-issuer"))
- tuple [rootd.rpki_key](#) = [rpki.x509.RSA](#)(Auto_file = [cfg.get](#)("rpki-key"))

- tuple `rootd.rpki_pkcs10_filename` = `cfg.get("rpki-pkcs10-filename", "")`
- tuple `rootd.rpki_subject_filename` = `cfg.get("rpki-subject-filename")`
- tuple `rootd.rpki_subject_lifetime` = `rpki.sundial.timedelta(days = 30)`
- `rootd.server_cert` = `rootd_bpki_cert`,

8.19 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`

8.20 rpkid.py File Reference

Namespaces

- namespace `rpkid`

Functions

- def `rpkid.main`

Variables

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

8.21 sql.py File Reference

Namespaces

- namespace `rpki.sql`

Classes

- class [rpki.sql.session](#)
- class [rpki.sql.sql_persistent](#)
- class [rpki.sql.template](#)

8.22 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](#)

8.23 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/"

8.24 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](#)

8.25 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`, 361
 - `__call__`
 - `irbe-cli::UsageWrapper`, 123
 - `rpki::https::Checker`, 179
 - `rpki::log::logger`, 242
 - `__cmp__`
 - `rpki::resource_set::resource_range`, 285
 - `rpki::resource_set::roa_prefix`, 310
 - `rpki::x509::DER_object`, 421
 - `__eq__`
 - `rpki::resource_set::resource_bag`, 282
 - `__init__`
 - `pubd::pubd_context`, 126
 - `rpki::config::parser`, 142
 - `rpki::https::Checker`, 179
 - `rpki::https::httpClient`, 181
 - `rpki::log::logger`, 242
 - `rpki::manifest::FileAndHash`, 243
 - `rpki::manifest::FilesAndHashes`, 244
 - `rpki::manifest::Manifest`, 245
 - `rpki::resource_set::resource_bag`, 282
 - `rpki::resource_set::resource_range`, 285
 - `rpki::resource_set::resource_set`, 295
 - `rpki::resource_set::roa_prefix`, 310
 - `rpki::resource_set::roa_prefix_set`, 315
 - `rpki::roa::ROAIPAddress`, 319
 - `rpki::roa::ROAIPAddresses`, 320
 - `rpki::roa::ROAIPAddressFamilies`, 321
 - `rpki::roa::ROAIPAddressFamily`, 322
 - `rpki::roa::RouteOriginAttestation`, 323
 - `rpki::rpki_engine::child_cert_obj`, 339
 - `rpki::rpki_engine::revoked_cert_obj`, 343
 - `rpki::rpki_engine::rpkid_context`, 346
 - `rpki::sql::session`, 350
 - `rpki::sql::template`, 359
 - `rpki::up_down::class_elt`, 373
 - `rpki::up_down::class_response_-syntax`, 377
 - `rpki::up_down::error_response_pdu`, 381
 - `rpki::up_down::multi_uri`, 395
 - `rpki::x509::DER_object`, 421
 - `rpki::x509::PEM_converter`, 426
 - `rpki::xml_utils::sax_handler`, 466
- `__init__.py(1882)`, 473
- `__ne__`
 - `rpki::resource_set::resource_bag`, 282
- `__new__`
 - `rpki::ipaddrs::v4addr`, 185
 - `rpki::ipaddrs::v6addr`, 187
- `__str__`
 - `rpki::ipaddrs::v4addr`, 185
 - `rpki::ipaddrs::v6addr`, 187
 - `rpki::resource_set::resource_bag`, 282
 - `rpki::resource_set::resource_range_-as`, 287
 - `rpki::resource_set::resource_range_-ip`, 289
 - `rpki::resource_set::resource_set`, 295
 - `rpki::resource_set::roa_prefix`, 310
 - `rpki::resource_set::roa_prefix_set`, 315
 - `rpki::sundial::datetime`, 361
 - `rpki::up_down::message_pdu`, 392
 - `rpki::up_down::multi_uri`, 395
 - `rpki::xml_utils::base_elt`, 455
 - `rpki::xml_utils::msg`, 463
- `__sub__`
 - `rpki::sundial::datetime`, 361
- `_bs2long`

- rpki::resource_set, 58
- _comm
 - rpki::resource_set::resource_set, 296
- _exceptions_enabled
 - rpki::sql::session, 352
- _long2bs
 - rpki::resource_set, 58
- _prefixlen
 - rpki::resource_set::resource_range_ip, 289
- _rsplit
 - rpki::resource_set, 58
- _wrap_execute
 - rpki::sql::session, 350
- activate
 - rpki::rpki_engine::ca_detail_obj, 327
- address
 - rpki::resource_set::roa_prefix, 311
 - rpki::roa::ROAIPAddress, 320
- addresses
 - rpki::roa::ROAIPAddressFamily, 322
- addressFamily
 - rpki::roa::ROAIPAddressFamily, 322
- afi
 - rpki::resource_set::resource_set_ipv4, 306
 - rpki::resource_set::resource_set_ipv6, 308
- argv
 - irbe-cli, 34
- as_number
 - irbe-cli::route_origin_elt, 119
 - rpki::left_right::route_origin_elt, 231
- asID
 - rpki::roa::RouteOriginAttestation, 324
- asn
 - rpki::left_right::list_resources_elt, 208
 - rpki::resource_set::resource_bag, 283
- assert_pristine
 - rpki::sql::session, 350
- attributes
 - rpki::left_right::bsc_elt, 191
 - rpki::left_right::child_elt, 196
 - rpki::left_right::list_resources_elt, 208
 - rpki::left_right::parent_elt, 216
 - rpki::left_right::report_error_elt, 219
 - rpki::left_right::repository_elt, 224
 - rpki::left_right::route_origin_elt, 231
 - rpki::left_right::self_elt, 240
 - rpki::publication::client_elt, 252
 - rpki::publication::config_elt, 259
 - rpki::publication::publication_object_elt, 274
 - rpki::publication::report_error_elt, 276
 - rpki::xml_utils::base_elt, 456
- b
 - rpki::x509::PEM_converter, 427
- base_uri
 - rpki::publication::client_elt, 252
- BaseHTTPServer::BaseHTTPRequestHandler, 67
- BaseHTTPServer::HTTPServer, 68
- bits
 - rpki::ipaddrs::v4addr, 186
 - rpki::ipaddrs::v6addr, 187
- booleans
 - rpki::left_right::bsc_elt, 191
 - rpki::left_right::child_elt, 196
 - rpki::left_right::parent_elt, 216
 - rpki::left_right::route_origin_elt, 231
 - rpki::left_right::self_elt, 240
 - rpki::xml_utils::base_elt, 456
- bpki_cert
 - irbe-cli::cmd_elt_mixin, 84
 - rpki::left_right::child_elt, 197
 - rpki::left_right::self_elt, 240
 - rpki::publication::client_elt, 252
- bpki_cms_cert
 - irbe-cli::cmd_elt_mixin, 84

- rpki::left_right::parent_elt, 216
- rpki::left_right::repository_elt, 224
- bpki_cms_glue
 - irbe-cli::cmd_elt_mixin, 84
 - rpki::left_right::parent_elt, 216
 - rpki::left_right::repository_elt, 225
- bpki_crl
 - irbe-cli::config_elt, 89
- bpki_glue
 - irbe-cli::cmd_elt_mixin, 85
 - rpki::left_right::child_elt, 197
 - rpki::left_right::self_elt, 240
 - rpki::publication::client_elt, 252
- bpki_https_cert
 - irbe-cli::cmd_elt_mixin, 85
 - rpki::left_right::parent_elt, 216
 - rpki::left_right::repository_elt, 225
- bpki_https_glue
 - irbe-cli::cmd_elt_mixin, 85
 - rpki::left_right::parent_elt, 216
 - rpki::left_right::repository_elt, 225
- bpki_ta
 - irbdb, 37
 - pubd::pubd_context, 127
 - rootd, 42
 - rpki::rpki_engine::rpkid_context, 347
- bsc
 - rpki::left_right::data_elt, 202
- bscs
 - rpki::left_right::self_elt, 238
- build
 - rpki::x509::ROA, 433
 - rpki::x509::SignedManifest, 442
- build_https_ta_cache
 - pubd::pubd_context, 126
 - rpki::https, 48
 - rpki::rpki_engine::rpkid_context, 346
- ca
 - rpki::rpki_engine::ca_detail_obj, 327
- ca_cert_uri
 - rpki::rpki_engine::ca_detail_obj, 330
- ca_detail
 - rpki::left_right::route_origin_elt, 229
 - rpki::rpki_engine::child_cert_obj, 339
 - rpki::rpki_engine::revoked_cert_obj, 343
- ca_detail_id
 - rpki::left_right::route_origin_elt, 231
 - rpki::rpki_engine::child_cert_obj, 340
 - rpki::rpki_engine::revoked_cert_obj, 344
- ca_details
 - rpki::rpki_engine::ca_obj, 333
- ca_from_class_name
 - rpki::left_right::child_elt, 195
- ca_id
 - rpki::rpki_engine::ca_detail_obj, 330
- cache
 - rpki::sql::session, 352
- cache_clear
 - rpki::sql::session, 351
- calculate_SKI
 - rpki::x509, 65
- call_daemon
 - irbe-cli, 34
- call_pubd
 - rpki::left_right::repository_elt, 223
- cas
 - rpki::left_right::parent_elt, 214
- cert
 - cross-certify, 31
 - rpki::left_right::route_origin_elt, 231
 - rpki::rpki_engine::child_cert_obj, 340
 - rpki::up_down::certificate_elt, 370
- cert_url
 - rpki::up_down::certificate_elt, 370
 - rpki::up_down::class_elt, 374
- certs
 - rpki::up_down::class_elt, 374
- cfg

- irbe-cli, 34
- irdbd, 37
- rootd, 42
- cfg_file
 - irbe-cli, 34
 - irdbd, 37
 - pubd, 40
 - rootd, 42
 - rpki, 67
- characters
 - rpki::xml_utils::sax_handler, 466
- check_allowed_uri
 - rpki::publication::client_elt, 251
- check_for_updates
 - rpki::rpki_engine::ca_obj, 333
- check_response
 - rpki::up_down::base_elt, 367
 - rpki::up_down::error_response_pdu, 381
 - rpki::up_down::issue_response_pdu, 387
- check_valid_rpki
 - rpki::x509::PKCS10, 429
- checker
 - rpki::https::httpsClient, 181
- child
 - cross-certify, 31
 - rpki::rpki_engine::child_cert_obj, 339
- child_bpki_cert
 - rootd, 42
- child_certs
 - rpki::left_right::child_elt, 195
 - rpki::rpki_engine::ca_detail_obj, 327
- child_id
 - rpki::rpki_engine::child_cert_obj, 341
- children
 - rpki::left_right::bsc_elt, 190
 - rpki::left_right::self_elt, 238
- class_name
 - rpki::up_down::class_elt, 374
 - rpki::up_down::issue_pdu, 385
 - rpki::up_down::revoke_pdu, 398
 - rpki::up_down::revoke_syntax, 402
- classes
 - rpki::up_down::class_response_syntax, 377
- clear
 - rpki::x509::DER_object, 421
- clear_https_ta_cache
 - pubd::pubd_context, 126
 - rpki::left_right::child_elt, 197
 - rpki::publication::client_elt, 252
 - rpki::rpki_engine::rpkiid_context, 346
- client
 - rpki::https, 48
- client_cert
 - irbe-cli, 35
- client_getopt
 - irbe-cli::cmd_elt_mixin, 83
- client_handler
 - pubd::pubd_context, 127
- client_key
 - irbe-cli, 35
- client_poll
 - rpki::left_right::self_elt, 238
- client_query_as_number
 - irbe-cli::route_origin_elt, 119
- client_query_bpki_cert
 - irbe-cli::cmd_elt_mixin, 83
- client_query_bpki_cms_cert
 - irbe-cli::cmd_elt_mixin, 83
- client_query_bpki_crl
 - irbe-cli::config_elt, 89
- client_query_bpki_https_cert
 - irbe-cli::cmd_elt_mixin, 83
- client_query_cms_glue
 - irbe-cli::cmd_elt_mixin, 83
- client_query_glue
 - irbe-cli::cmd_elt_mixin, 84
- client_query_https_glue
 - irbe-cli::cmd_elt_mixin, 84
- client_query_ipv4
 - irbe-cli::route_origin_elt, 119
- client_query_ipv6
 - irbe-cli::route_origin_elt, 119
- client_query_signing_cert
 - irbe-cli::bsc_elt, 72
- client_query_signing_cert_crl

- irbe-cli::bsc_elt, 72
- client_reply_decode
 - irbe-cli::bsc_elt, 72
 - irbe-cli::cmd_elt_mixin, 84
- client_reply_show
 - irbe-cli::cmd_elt_mixin, 84
- client_ta
 - irdbd, 37
 - rootd, 42
- close
 - rpki::sql::session, 351
- cms_class
 - irbe-cli, 35
- codes
 - rpki::up_down::error_response_pdu, 382
- columns
 - rpki::sql::template, 359
- compose_response
 - rootd, 41
- config.py(1873), 473
- config_id
 - rpki::publication::config_elt, 259
- ConfigParser::RawConfigParser, 68
- connect
 - rpki::sql::session, 351
- construct_sia_uri
 - rpki::rpki_engine::ca_obj, 334
- contains
 - rpki::resource_set::resource_set, 296
- content
 - rpki::x509::CMS_object, 410
 - rpki::x509::DER_CMS_object, 417
 - rpki::x509::XML_CMS_object, 452
- content_class
 - rpki::x509::ROA, 433
 - rpki::x509::SignedManifest, 442
- control_handler
 - pubd::pubd_context, 127
- convert_to_seconds
 - rpki::sundial::timedelta, 365
- create
 - rpki::rpki_engine::ca_detail_obj, 327
 - rpki::rpki_engine::ca_obj, 334
 - rpki::x509::PKCS10, 429
- create_ca
 - rpki::x509::PKCS10, 429
- create_top_level
 - rpki::xml_utils::sax_handler, 466
- crl_interval
 - rpki::left_right::self_elt, 240
- crl_uri
 - rpki::rpki_engine::ca_detail_obj, 327
- cronjob_handler
 - rpki::rpki_engine::rpkid_context, 346
- cross, 30
- cross-certify, 31
 - cert, 31
 - child, 31
 - f, 31
 - keypair, 31
 - lifetime, 32
 - notAfter, 32
 - now, 32
 - output, 32
 - parent, 32
 - serial, 32
 - serial_file, 32
 - usage, 31
 - x, 32
- cross-certify.py(1880), 473
- cur
 - irdbd, 37
 - rpki::sql::session, 352
- database
 - rpki::sql::session, 352
- datum_type
 - rpki::resource_set::resource_range_as, 287
 - rpki::resource_set::resource_range_ipv4, 291
 - rpki::resource_set::resource_range_ipv6, 293
- db
 - irdbd, 38
 - rpki::sql::session, 352
- debug
 - rpki::log, 52

- debug_cms_certs
 - rpki::x509::CMS_object, 410
- debug_tls_certs
 - rpki::https, 49
- decode
 - rpki::x509::DER_CMS_object, 417
 - rpki::x509::XML_CMS_object, 451
- default_section
 - rpki::config::parser, 142
- del_subject_cert
 - rootd, 41
- delete
 - rpki::rpki_engine::ca_detail_obj, 327
 - rpki::rpki_engine::ca_obj, 334
 - rpki::sql::template, 359
- DER
 - rpki::x509::CMS_object, 410
 - rpki::x509::CRL, 414
 - rpki::x509::DER_object, 424
 - rpki::x509::PKCS10, 430
 - rpki::x509::RSA, 437
 - rpki::x509::RSAPublic, 440
 - rpki::x509::X509, 447
- description
 - rpki::up_down::error_response_pdu, 382
- difference
 - rpki::resource_set::resource_set, 296
- dirty
 - rpki::sql::session, 352
- disable_tls_certificate_validation_exceptions
 - rpki::https, 49
- do_POST
 - rpki::https::requestHandler, 184
- dump_inbound_cms
 - rpki::x509::XML_CMS_object, 452
- dump_on_verify_failure
 - rpki::x509::CMS_object, 410
- dump_outbound_cms
 - rpki::x509::XML_CMS_object, 453
- dump_to_disk
 - rpki::x509::XML_CMS_object, 451
- dumpasn1
 - rpki::x509::DER_object, 421
- dynamic_https_trust_anchor
 - rpki::https::Checker, 180
- e
 - rpki::x509::PEM_converter, 427
- earlier
 - rpki::sundial::datetime, 362
- econtent_oid
 - rpki::x509::CMS_object, 410
 - rpki::x509::ROA, 433
 - rpki::x509::SignedManifest, 442
 - rpki::x509::XML_CMS_object, 453
- ee_uri
 - rpki::left_right::route_origin_elt, 229
- ee_uri_tail
 - rpki::left_right::route_origin_elt, 229
- element_name
 - rpki::left_right::bsc_elt, 191
 - rpki::left_right::child_elt, 197
 - rpki::left_right::list_resources_elt, 208
 - rpki::left_right::parent_elt, 216
 - rpki::left_right::report_error_elt, 219
 - rpki::left_right::repository_elt, 225
 - rpki::left_right::route_origin_elt, 232
 - rpki::left_right::self_elt, 240
 - rpki::publication::certificate_elt, 248
 - rpki::publication::client_elt, 253
 - rpki::publication::config_elt, 259
 - rpki::publication::crl_elt, 265
 - rpki::publication::manifest_elt, 267
 - rpki::publication::report_error_elt, 276
 - rpki::publication::roa_elt, 278
- elements
 - rpki::left_right::bsc_elt, 191
 - rpki::left_right::child_elt, 197
 - rpki::left_right::parent_elt, 216
 - rpki::left_right::repository_elt, 225
 - rpki::left_right::self_elt, 241
 - rpki::publication::client_elt, 253
 - rpki::publication::config_elt, 259
 - rpki::xml_utils::base_elt, 457

- empty
 - rpki::resource_set::resource_bag, 282
 - rpki::x509::DER_object, 421
- enable_trace
 - rpki::log, 52
- encode
 - rpki::x509::DER_CMS_object, 417
 - rpki::x509::XML_CMS_object, 451
- encoding
 - rpki::left_right::cms_msg, 199
 - rpki::publication::cms_msg, 255
 - rpki::up_down::cms_msg, 379
- endElement
 - rpki::left_right::child_elt, 196
 - rpki::publication::client_elt, 251
 - rpki::publication::publication_object_elt, 273
 - rpki::up_down::base_elt, 367
 - rpki::up_down::certificate_elt, 370
 - rpki::up_down::class_elt, 373
 - rpki::up_down::error_response_pdu, 381
 - rpki::up_down::issue_pdu, 384
 - rpki::xml_utils::base_elt, 455
 - rpki::xml_utils::data_elt, 459
 - rpki::xml_utils::msg, 463
 - rpki::xml_utils::sax_handler, 467
- endElementNS
 - rpki::xml_utils::sax_handler, 467
- enforce_strict_up_down_xml_sender
 - rpki::left_right, 50
- error
 - rpki::log, 52
- error_code
 - rpki::left_right::report_error_elt, 219
 - rpki::publication::report_error_elt, 276
- Exception, 69
- exceptions
 - rpki::up_down::error_response_pdu, 382
- exceptions.py(1873), 474
- excludes
 - irbe-cli::bsc_elt, 73
 - irbe-cli::cmd_elt_mixin, 85
- execute
 - rpki::sql::session, 351
- executemany
 - rpki::sql::session, 351
- expires
 - rpki::rpki_engine::revoked_cert_obj, 344
- explicitVersion
 - rpki::manifest::Manifest, 246
 - rpki::roa::RouteOriginAttestation, 324
- f
 - cross-certify, 31
- fetch
 - rpki::publication::config_elt, 258
 - rpki::rpki_engine::child_cert_obj, 339
- fetch_active
 - rpki::rpki_engine::ca_obj, 334
- fetch_deprecated
 - rpki::rpki_engine::ca_obj, 334
- fetch_pending
 - rpki::rpki_engine::ca_obj, 335
- fetch_revoked
 - rpki::rpki_engine::ca_obj, 335
- fetchall
 - rpki::sql::session, 351
- file
 - rpki::manifest::FileAndHash, 244
- fileHashAlg
 - rpki::manifest::Manifest, 246
- fileList
 - rpki::manifest::Manifest, 246
- formats
 - rpki::x509::CMS_object, 411
 - rpki::x509::CRL, 414
 - rpki::x509::DER_object, 424
 - rpki::x509::PKCS10, 430
 - rpki::x509::RSA, 437
 - rpki::x509::RSAPublic, 440
 - rpki::x509::X509, 447
- from_exception
 - rpki::left_right::report_error_elt, 219
 - rpki::publication::report_error_elt, 276

- from_resource_bag
 - rpki::up_down::class_elt, [373](#)
- from_rfc3779_tuples
 - rpki::resource_set::resource_bag, [282](#)
- from_sql
 - rpki::resource_set::resource_set, [296](#)
 - rpki::resource_set::roa_prefix_set, [315](#)
 - rpki::sundial::datetime, [362](#)
 - rpki::x509::DER_object, [421](#)
- fromASN1tuple
 - rpki::sundial::datetime, [362](#)
- fromdatetime
 - rpki::sundial::datetime, [362](#)
- fromGeneralizedTime
 - rpki::sundial::datetime, [362](#)
- fromUTCTime
 - rpki::sundial::datetime, [362](#)
- fromXMLtime
 - rpki::sundial::datetime, [362](#)
- gAKI
 - rpki::x509::DER_object, [422](#)
- gctx
 - rpki::rpki_engine::ca_detail_obj, [330](#)
 - rpki::rpki_engine::ca_obj, [336](#)
 - rpki::rpki_engine::child_cert_obj, [341](#)
 - rpki::rpki_engine::revoked_cert_obj, [344](#)
 - rpki::sql::sql_persistent, [357](#)
- generate
 - rpki::x509::CRL, [413](#)
 - rpki::x509::RSA, [435](#)
- generate_crl
 - rpki::rpki_engine::ca_detail_obj, [327](#)
- generate_manifest
 - rpki::rpki_engine::ca_detail_obj, [328](#)
- generate_manifest_cert
 - rpki::rpki_engine::ca_detail_obj, [328](#)
- generate_roa
 - rpki::left_right::route_origin_elt, [229](#)
- get
 - rpki::config::parser, [142](#)
- get_3779resources
 - rpki::x509::DER_object, [422](#)
- get_AIA
 - rpki::x509::DER_object, [422](#)
- get_AKI
 - rpki::x509::DER_object, [422](#)
- get_Base64
 - rpki::x509::DER_object, [422](#)
- get_basicConstraints
 - rpki::x509::DER_object, [422](#)
- get_content
 - rpki::x509::CMS_object, [409](#)
- get_DER
 - rpki::x509::CMS_object, [409](#)
 - rpki::x509::CRL, [413](#)
 - rpki::x509::DER_object, [422](#)
 - rpki::x509::PKCS10, [430](#)
 - rpki::x509::RSA, [435](#)
 - rpki::x509::RSAPublic, [439](#)
 - rpki::x509::X509, [445](#)
- get_PEM
 - rpki::x509::DER_object, [423](#)
- get_POW
 - rpki::x509::CMS_object, [409](#)
 - rpki::x509::CRL, [413](#)
 - rpki::x509::RSA, [436](#)
 - rpki::x509::RSAPublic, [439](#)
 - rpki::x509::X509, [446](#)
- get_POWpkix
 - rpki::x509::CRL, [414](#)
 - rpki::x509::PKCS10, [430](#)
 - rpki::x509::X509, [446](#)
- get_public_DER
 - rpki::x509::RSA, [436](#)
- get_RSAPublic
 - rpki::x509::RSA, [436](#)
- get_SIA
 - rpki::x509::DER_object, [423](#)
- get_SKI
 - rpki::up_down::revoke_pdu, [398](#)
 - rpki::x509::DER_object, [423](#)
 - rpki::x509::RSA, [436](#)

- rpki::x509::RSAPublic, 439
- get_subject_cert
 - rootd, 42
- get_tslite
 - rpki::x509::RSA, 436
 - rpki::x509::X509, 446
- getIssuer
 - rpki::x509::CRL, 414
 - rpki::x509::X509, 446
- getNextUpdate
 - rpki::x509::CRL, 414
 - rpki::x509::SignedManifest, 442
- getNotAfter
 - rpki::x509::X509, 446
- getNotBefore
 - rpki::x509::X509, 446
- getPublicKey
 - rpki::x509::PKCS10, 430
 - rpki::x509::X509, 446
- getSerial
 - rpki::x509::X509, 447
- getSubject
 - rpki::x509::X509, 447
- getThisUpdate
 - rpki::x509::CRL, 414
 - rpki::x509::SignedManifest, 442
- gSKI
 - rpki::x509::DER_object, 423
- hAKI
 - rpki::x509::DER_object, 423
- handler
 - irdbd, 37
- handler_common
 - pubd::pubd_context, 127
- handlers
 - irdbd, 38
 - rootd, 42
- handshake
 - rpki::https::httpsServer, 182
- hash
 - rpki::manifest::FileAndHash, 244
- host
 - irdbd, 38
 - rootd, 43
- hSKI
 - rpki::x509::DER_object, 423
- https.py(1873), 475
- https_server_host
 - pubd::pubd_context, 127
 - rootd, 43
 - rpki::rpki_engine::rpkid_context, 347
- https_server_port
 - pubd::pubd_context, 127
 - rootd, 43
 - rpki::rpki_engine::rpkid_context, 347
- https_ta_cache
 - pubd::pubd_context, 127
 - rpki::rpki_engine::rpkid_context, 347
- index
 - rpki::sql::template, 359
- info
 - rpki::log, 52
- inherit
 - rpki::resource_set::resource_set, 297
 - rpki::resource_set::resource_set_as, 300
 - rpki::resource_set::resource_set_ip, 304
- inherit_token
 - rpki::resource_set, 59
- init
 - rpki::log, 51
- insert
 - rpki::sql::template, 359
- intersection
 - rpki::resource_set::resource_bag, 282
 - rpki::resource_set::resource_set, 296
- ipAddrBlocks
 - rpki::roa::RouteOriginAttestation, 324
- ipaddrs.py(1873), 475
- ipv4
 - irbe-cli::route_origin_elt, 119
 - rpki::left_right::list_resources_elt, 208

- rpki::left_right::route_origin_elt, 232
- ipv6
 - irbe-cli::route_origin_elt, 120
 - rpki::left_right::list_resources_elt, 208
 - rpki::left_right::route_origin_elt, 232
- irbe, 32
- irbe-cli, 33
 - argv, 34
 - call_daemon, 34
 - cfg, 34
 - cfg_file, 34
 - client_cert, 35
 - client_key, 35
 - cms_class, 35
 - pem_out, 35
 - q_msg, 35
 - q_msg_left_right, 35
 - q_msg_publication, 35
 - q_pdu, 35
 - server_ta, 35
 - top_opts, 35
 - url, 36
 - usage, 34
 - usage_fill, 36
 - verbose, 36
- irbe-cli.py(1880), 476
- irbe-cli::bsc_elt, 71
 - client_query_signing_cert, 72
 - client_query_signing_cert_crl, 72
 - client_reply_decode, 72
 - excludes, 73
 - signing_cert, 73
 - signing_cert_crl, 73
- irbe-cli::certificate_elt, 75
- irbe-cli::child_elt, 78
- irbe-cli::client_elt, 81
- irbe-cli::cmd_elt_mixin, 82
 - bpki_cert, 84
 - bpki_cms_cert, 84
 - bpki_cms_glue, 84
 - bpki_glue, 85
 - bpki_https_cert, 85
 - bpki_https_glue, 85
 - client_getopt, 83
 - client_query_bpki_cert, 83
 - client_query_bpki_cms_cert, 83
 - client_query_bpki_https_cert, 83
 - client_query_cms_glue, 83
 - client_query_glue, 84
 - client_query_https_glue, 84
 - client_reply_decode, 84
 - client_reply_show, 84
 - excludes, 85
 - usage, 84
- irbe-cli::cmd_msg_mixin, 86
 - usage, 86
- irbe-cli::config_elt, 88
 - bpki_crl, 89
 - client_query_bpki_crl, 89
- irbe-cli::crl_elt, 91
- irbe-cli::left_right_cms_msg, 93
 - saxify, 94
- irbe-cli::left_right_msg, 95
 - pdu, 96
- irbe-cli::left_right_sax_handler, 97
 - pdu, 98
- irbe-cli::manifest_elt, 100
- irbe-cli::parent_elt, 103
- irbe-cli::publication_cms_msg, 105
 - saxify, 106
- irbe-cli::publication_msg, 107
 - pdu, 108
- irbe-cli::publication_sax_handler, 109
 - pdu, 110
- irbe-cli::repository_elt, 112
- irbe-cli::roa_elt, 115
- irbe-cli::route_origin_elt, 118
 - as_number, 119
 - client_query_as_number, 119
 - client_query_ipv4, 119
 - client_query_ipv6, 119
 - ipv4, 119
 - ipv6, 120
- irbe-cli::self_elt, 122
- irbe-cli::UsageWrapper, 123
 - __call__, 123
- irbe_cert
 - pubd::pubd_context, 127

- rpki::rpki_engine::rpkid_context, 348
- irdb_cert
 - rpki::rpki_engine::rpkid_context, 348
- irdb_query
 - rpki::rpki_engine::rpkid_context, 346
- irdb_url
 - rpki::rpki_engine::rpkid_context, 348
- irdbd, 36
 - bpki_ta, 37
 - cfg, 37
 - cfg_file, 37
 - client_ta, 37
 - cur, 37
 - db, 38
 - handler, 37
 - handlers, 38
 - host, 38
 - irdbd_cert, 38
 - irdbd_key, 38
 - port, 38
 - rpkid_cert, 38
 - server_cert, 38
 - startup_msg, 38
 - u, 39
- irdbd.py(1880), 477
- irdbd_cert
 - irdbd, 38
- irdbd_key
 - irdbd, 38
- is_CA
 - rpki::x509::DER_object, 424
- issubset
 - rpki::resource_set::resource_set, 297
- issue
 - rpki::rpki_engine::ca_detail_obj, 328
 - rpki::x509::X509, 447
- issue_ee
 - rpki::rpki_engine::ca_detail_obj, 328
- issuer
 - rpki::up_down::class_elt, 374
- issuperset
 - rpki::resource_set::resource_set, 297
- keypair
 - cross-certify, 31
- last_crl_sn
 - rpki::rpki_engine::ca_obj, 336
- last_issued_sn
 - rpki::rpki_engine::ca_obj, 336
- last_manifest_sn
 - rpki::rpki_engine::ca_obj, 336
- lastrowid
 - rpki::sql::session, 351
- later
 - rpki::sundial::datetime, 363
- latest_ca_cert
 - rpki::rpki_engine::ca_detail_obj, 330
- latest_crl
 - rpki::rpki_engine::ca_detail_obj, 330
- latest_manifest
 - rpki::rpki_engine::ca_detail_obj, 330
- latest_manifest_cert
 - rpki::rpki_engine::ca_detail_obj, 330
- left_right
 - rpki::relaxng, 56
- left_right.py(1873), 478
- left_right_handler
 - rpki::rpki_engine::rpkid_context, 347
- lifetime
 - cross-certify, 32
- list, 124
- log.py(1873), 478
- log_message
 - rpki::https::requestHandler, 184
- long, 124
- looks_like_PEM
 - rpki::x509::PEM_converter, 426
- main
 - pubd, 40

- rpkiid, 67
- make_b64elt
 - rpki::up_down::base_elt, 367
 - rpki::xml_utils::base_elt, 455
- make_elt
 - rpki::up_down::base_elt, 367
 - rpki::xml_utils::base_elt, 455
- make_pdu
 - rpki::xml_utils::base_elt, 455
- make_prefix
 - rpki::resource_set::resource_range - ip, 289
- make_query
 - rpki::up_down::message_pdu, 392
- make_reply
 - rpki::xml_utils::data_elt, 459
- make_reply_clone_hook
 - rpki::left_right::data_elt, 202
 - rpki::xml_utils::data_elt, 459
- manifest.py(1873), 479
- manifest_private_key_id
 - rpki::rpki_engine::ca_detail_obj, 330
- manifest_public_key
 - rpki::rpki_engine::ca_detail_obj, 330
- manifest_uri
 - rpki::rpki_engine::ca_detail_obj, 328
- manifestNumber
 - rpki::manifest::Manifest, 246
- map
 - rpki::sql::template, 359
- max
 - rpki::resource_set::resource_range, 285
 - rpki::resource_set::roa_prefix, 310
- max_prefixlen
 - rpki::resource_set::roa_prefix, 311
- maxLength
 - rpki::roa::ROAIPAddress, 320
- min
 - rpki::resource_set::resource_range, 285
 - rpki::resource_set::resource_range - as, 287
 - rpki::resource_set::roa_prefix, 310
- multiget
 - rpki::config::parser, 142
- name
 - rpki::left_right::sax_handler, 234
 - rpki::publication::sax_handler, 280
 - rpki::up_down::sax_handler, 405
- name2oid
 - rpki::oids, 54
- name2type
 - rootd::message_pdu, 137
 - rpki::up_down::message_pdu, 393
- next_crl_number
 - rpki::rpki_engine::ca_obj, 335
- next_manifest_number
 - rpki::rpki_engine::ca_obj, 335
- next_serial_number
 - rpki::rpki_engine::ca_obj, 335
- nextUpdate
 - rpki::manifest::Manifest, 246
- normalize_chain
 - rpki::x509::X509, 447
- notAfter
 - cross-certify, 32
- note
 - rpki::log, 52
- now
 - cross-certify, 32
 - rpki::sundial, 62
- nsmap
 - rpki::left_right::left_right - namespace, 205
 - rpki::publication::publication - namespace, 271
 - rpki::up_down, 64
- obj2elt
 - rpki::publication, 56
- object, 125
- object_delete
 - rpki::left_right::repository_elt, 223
- object_write
 - rpki::left_right::repository_elt, 224
- oid2name
 - rpki::oids, 54

- oids.py(1873), 479
- other_clear
 - rpki::x509::CMS_object, 411
 - rpki::x509::DER_object, 425
- output
 - cross-certify, 32
- oversized
 - rpki::resource_set::resource_bag, 283
- parent
 - cross-certify, 32
 - rpki::rpki_engine::ca_obj, 335
- parent_id
 - rpki::rpki_engine::ca_obj, 336
- parent_resource_class
 - rpki::rpki_engine::ca_obj, 336
- parents
 - rpki::left_right::bsc_elt, 190
 - rpki::left_right::child_elt, 196
 - rpki::left_right::repository_elt, 224
 - rpki::left_right::self_elt, 238
- parse
 - rpki::sundial::timedelta, 365
- parse_rfc3779_tuple
 - rpki::resource_set::resource_set_as, 299
 - rpki::resource_set::resource_set_ip, 303
- parse_str
 - rpki::resource_set::resource_set_as, 299
 - rpki::resource_set::resource_set_ip, 303
 - rpki::resource_set::roa_prefix_set, 315
- password
 - rpki::sql::session, 352
- payload
 - rpki::publication::publication_object_elt, 274
 - rpki::up_down::message_pdu, 393
- payload_type
 - rpki::publication::certificate_elt, 248
 - rpki::publication::crl_elt, 265
 - rpki::publication::manifest_elt, 267
 - rpki::publication::roa_elt, 278
- pdu
 - irbe-cli::left_right_sax_handler, 98
 - irbe-cli::publication_sax_handler, 110
 - rootd::sax_handler, 141
 - rpki::left_right::sax_handler, 234
 - rpki::publication::sax_handler, 280
 - rpki::up_down::sax_handler, 405
- pdu_s
 - irbe-cli::left_right_msg, 96
 - irbe-cli::publication_msg, 108
 - rpki::left_right::msg, 210
 - rpki::publication::msg, 269
- pem_converter
 - rpki::x509::CRL, 415
 - rpki::x509::DER_object, 425
 - rpki::x509::PKCS10, 430
 - rpki::x509::ROA, 433
 - rpki::x509::RSA, 437
 - rpki::x509::RSAPublic, 440
 - rpki::x509::SignedManifest, 443
 - rpki::x509::X509, 448
- pem_dump_tls_certs
 - rpki::https::Checker, 180
- pem_out
 - irbe-cli, 35
- ping
 - rpki::sql::session, 351
- pkcs10
 - rpki::up_down::issue_pdu, 385
- pkcs10_request
 - rpki::left_right::bsc_elt, 192
- PKIX_threshold
 - rpki::sundial::datetime, 364
- port
 - irdbd, 38
 - rootd, 43
- POW
 - rpki::x509::CMS_object, 411
 - rpki::x509::CRL, 415
 - rpki::x509::RSA, 437
 - rpki::x509::RSAPublic, 440
 - rpki::x509::X509, 448
- POWify_OID
 - rpki::x509, 65

- POWpkix
 - rpki::x509::CRL, 415
 - rpki::x509::PKCS10, 431
 - rpki::x509::X509, 448
- prefix_type
 - rpki::resource_set::roa_prefix_set_
 ipv4, 317
 - rpki::resource_set::roa_prefix_set_
 ipv6, 318
- prefixlen
 - rpki::resource_set::roa_prefix, 311
- pretty_print_content
 - rpki::x509::XML_CMS_object, 452
- print_on_der_error
 - rpki::x509::CMS_object, 411
- priority
 - rpki::log::logger, 243
- private_key_id
 - rpki::left_right::bsc_elt, 192
 - rpki::rpki_engine::ca_detail_obj,
 330
- profile
 - pubd, 40
 - rpkid, 67
- pubd, 39
 - cfg_file, 40
 - main, 40
 - profile, 40
- pubd.py(1880), 480
- pubd::pubd_context, 125
 - __init__, 126
 - bpki_ta, 127
 - build_https_ta_cache, 126
 - clear_https_ta_cache, 126
 - client_handler, 127
 - control_handler, 127
 - handler_common, 127
 - https_server_host, 127
 - https_server_port, 127
 - https_ta_cache, 127
 - irbe_cert, 127
 - pubd_cert, 128
 - pubd_key, 128
 - publication_base, 128
 - sql, 128
- pubd_cert
 - pubd::pubd_context, 128
- pubd_key
 - pubd::pubd_context, 128
- public_key
 - rpki::rpki_engine::ca_detail_obj,
 330
- publication
 - rpki::relaxng, 56
- publication.py(1873), 480
- publication_base
 - pubd::pubd_context, 128
- publication_kludge_base
 - rpki::rpki_engine::rpkid_context,
 348
- publish
 - rpki::left_right::repository_elt, 224
- pydatetime::datetime, 129
- pydatetime::timedelta, 129
- q_msg
 - irbe-cli, 35
- q_msg_left_right
 - irbe-cli, 35
- q_msg_publication
 - irbe-cli, 35
- q_pdu
 - irbe-cli, 35
- query
 - rpki::up_down::issue_pdu, 384
 - rpki::up_down::list_pdu, 389
 - rpki::up_down::revoke_pdu, 398
- query_up_down
 - rpki::left_right::parent_elt, 214
- range_type
 - rpki::resource_set::resource_set_as,
 300
 - rpki::resource_set::resource_set_
 ipv4, 306
 - rpki::resource_set::resource_set_
 ipv6, 308
 - rpki::resource_set::roa_prefix_ipv4,
 312
 - rpki::resource_set::roa_prefix_ipv6,
 314
- read_attrs

- rpki::xml_utils::base_elt, 456
- recipient
 - rpki::up_down::message_pdu, 394
- refuse_tls_ca_certs
 - rpki::https::Checker, 180
- regen_margin
 - rpki::left_right::self_elt, 241
- regenerate_crls_and_manifests
 - rpki::left_right::self_elt, 238
- regenerate_roa
 - rpki::left_right::route_origin_elt, 229
- regex
 - rpki::sundial::timedelta, 365
- reissue
 - rpki::rpki_engine::child_cert_obj, 340
- rekey
 - rpki::rpki_engine::ca_obj, 335
- relaxng.py(1838), 481
- repositories
 - rpki::left_right::bsc_elt, 191
 - rpki::left_right::self_elt, 238
- repository
 - rpki::left_right::parent_elt, 215
- req_resource_set_as
 - rpki::up_down::certificate_elt, 371
 - rpki::up_down::issue_pdu, 385
- req_resource_set_ipv4
 - rpki::up_down::certificate_elt, 371
 - rpki::up_down::issue_pdu, 385
- req_resource_set_ipv6
 - rpki::up_down::certificate_elt, 371
 - rpki::up_down::issue_pdu, 385
- require_crls
 - rpki::x509::CMS_object, 411
- resource_set.py(1873), 481
- resource_set_as
 - rpki::up_down::class_elt, 374
- resource_set_ipv4
 - rpki::up_down::class_elt, 375
- resource_set_ipv6
 - rpki::up_down::class_elt, 375
- resource_set_notafter
 - rpki::up_down::class_elt, 375
- resource_set_type
 - rpki::resource_set::roa_prefix_set_ipv4, 317
 - rpki::resource_set::roa_prefix_set_ipv6, 318
- result
 - rpki::xml_utils::sax_handler, 468
- revoke
 - rpki::rpki_engine::ca_detail_obj, 328
 - rpki::rpki_engine::ca_obj, 336
 - rpki::rpki_engine::child_cert_obj, 340
 - rpki::rpki_engine::revoked_cert_obj, 343
- revoked
 - rpki::rpki_engine::revoked_cert_obj, 344
- revoked_certs
 - rpki::rpki_engine::ca_detail_obj, 329
- roa
 - rpki::left_right::route_origin_elt, 232
- roa.py(1873), 482
- roa_uri
 - rpki::left_right::route_origin_elt, 229
- rootd, 40
 - bpki_ta, 42
 - cfg, 42
 - cfg_file, 42
 - child_bpki_cert, 42
 - client_ta, 42
 - compose_response, 41
 - del_subject_cert, 41
 - get_subject_cert, 42
 - handlers, 42
 - host, 43
 - https_server_host, 43
 - https_server_port, 43
 - port, 43
 - rootd_base, 43
 - rootd_bpki_cert, 43
 - rootd_bpki_crl, 43
 - rootd_bpki_key, 43
 - rootd_cert, 43

- rootd_name, 43
- rpki_issuer, 44
- rpki_key, 44
- rpki_pkcs10_filename, 44
- rpki_subject_filename, 44
- rpki_subject_lifetime, 44
- server_cert, 44
- set_subject_cert, 42
- stash_subject_pkcs10, 42
- up_down_handler, 42
- rootd.py(1880), 482
- rootd::cms_msg, 130
 - saxify, 131
- rootd::issue_pdu, 132
 - serve_pdu, 133
- rootd::list_pdu, 134
 - serve_pdu, 135
- rootd::message_pdu, 136
 - name2type, 137
 - type2name, 137
- rootd::revoke_pdu, 138
 - serve_pdu, 139
- rootd::sax_handler, 140
 - pdu, 141
- rootd_base
 - rootd, 43
- rootd_bpki_cert
 - rootd, 43
- rootd_bpki_crl
 - rootd, 43
- rootd_bpki_key
 - rootd, 43
- rootd_cert
 - rootd, 43
- rootd_name
 - rootd, 43
- route_origins
 - rpki::left_right::self_elt, 238
 - rpki::rpki_engine::ca_detail_obj, 329
- rpki, 44
- rpki.config, 45
- rpki.exceptions, 45
- rpki.https, 47
- rpki.ipaddrs, 49
- rpki.left_right, 50
- rpki.log, 51
- rpki.manifest, 53
- rpki.oids, 53
- rpki.publication, 55
- rpki.relaxng, 56
- rpki.resource_set, 57
- rpki.roa, 59
- rpki.rpki_engine, 60
- rpki.sql, 61
- rpki.sundial, 62
- rpki.up_down, 63
- rpki.x509, 64
- rpki.xml_utils, 65
- rpki::config::parser, 141
 - __init__, 142
 - default_section, 142
 - get, 142
 - multiget, 142
- rpki::exceptions::BadClassNameSyntax, 143
- rpki::exceptions::BadContactURL, 144
- rpki::exceptions::BadIRDBReply, 145
- rpki::exceptions::BadIssueResponse, 146
- rpki::exceptions::BadPKCS10, 147
- rpki::exceptions::BadQuery, 148
- rpki::exceptions::BadSender, 149
- rpki::exceptions::BadStatusCode, 150
- rpki::exceptions::BadURISyntax, 151
- rpki::exceptions::BSCNotFound, 152
- rpki::exceptions::ChildNotFound, 153
- rpki::exceptions::ClassNameMismatch, 154
- rpki::exceptions::CMSCRLNotSet, 155
- rpki::exceptions::CMSVerificationFailed, 156
- rpki::exceptions::DBConsistencyError, 157
- rpki::exceptions::DERObjectConversionError, 158
- rpki::exceptions::EmptyPEM, 159
- rpki::exceptions::HTTPRequestFailed, 160
- rpki::exceptions::MissingCMSCRL, 161
- rpki::exceptions::MissingCMSEECert, 162

- rpki::exceptions::MultipleTLSEECert, 163
- rpki::exceptions::MustBePrefix, 164
- rpki::exceptions::NotACertificateChain, 165
- rpki::exceptions::NotFound, 166
- rpki::exceptions::NotImplementedYet, 167
- rpki::exceptions::NotInDatabase, 168
- rpki::exceptions::ReceivedTLSCACert, 169
- rpki::exceptions::RPKI_Exception, 169
- rpki::exceptions::ServerShuttingDown, 170
- rpki::exceptions::SKIMismatch, 171
- rpki::exceptions::SubprocessError, 172
- rpki::exceptions::TLSValidationError, 173
- rpki::exceptions::UnexpectedCMSCerts, 174
- rpki::exceptions::UnexpectedCMSCRLs, 175
- rpki::exceptions::UnparsableCMSDER, 176
- rpki::exceptions::UpstreamError, 177
- rpki::exceptions::WrongContentType, 178
- rpki::https
 - build_https_ta_cache, 48
 - client, 48
 - debug_tls_certs, 49
 - disable_tls_certificate_validation_exceptions, 49
 - rpki_content_type, 49
 - server, 48
 - tlslite_certChain, 48
- rpki::https::Checker, 178
 - __call__, 179
 - __init__, 179
 - dynamic_https_trust_anchor, 180
 - pem_dump_tls_certs, 180
 - refuse_tls_ca_certs, 180
 - x509store, 180
 - x509store_thunk, 179
- rpki::https::httpsClient, 180
 - __init__, 181
 - checker, 181
- rpki::https::httpsServer, 182
 - handshake, 182
 - rpki_checker, 183
 - rpki_server_cert, 183
 - rpki_server_key, 183
 - rpki_sessionCache, 183
- rpki::https::requestHandler, 183
 - do_POST, 184
 - log_message, 184
 - rpki_find_handler, 184
 - rpki_handlers, 184
- rpki::ipaddrs::v4addr, 185
 - __new__, 185
 - __str__, 185
 - bits, 186
- rpki::ipaddrs::v6addr, 186
 - __new__, 187
 - __str__, 187
 - bits, 187
- rpki::left_right
 - enforce_strict_up_down_xml_sender, 50
- rpki::left_right::bsc_elt, 189
 - attributes, 191
 - booleans, 191
 - children, 190
 - element_name, 191
 - elements, 191
 - parents, 190
 - pkcs10_request, 192
 - private_key_id, 192
 - repositories, 191
 - serve_pre_save_hook, 191
 - signing_cert, 192
 - signing_cert_crl, 192
 - sql_template, 192
- rpki::left_right::child_elt, 194
 - attributes, 196
 - booleans, 196
 - bpki_cert, 197
 - bpki_glue, 197
 - ca_from_class_name, 195
 - child_certs, 195
 - clear_https_ta_cache, 197
 - element_name, 197

- elements, [197](#)
- endElement, [196](#)
- parents, [196](#)
- serve_post_save_hook, [196](#)
- serve_up_down, [196](#)
- sql_template, [197](#)
- rpki::left_right::cms_msg, [198](#)
 - encoding, [199](#)
 - saxify, [199](#)
 - schema, [199](#)
- rpki::left_right::data_elt, [201](#)
 - bsc, [202](#)
 - make_reply_clone_hook, [202](#)
 - self, [202](#)
 - serve_fetch_all, [202](#)
 - serve_fetch_one, [202](#)
 - unimplemented_control, [203](#)
- rpki::left_right::left_right_namespace, [204](#)
 - nsmmap, [205](#)
 - xmlns, [205](#)
- rpki::left_right::list_resources_elt, [206](#)
 - asn, [208](#)
 - attributes, [208](#)
 - element_name, [208](#)
 - ipv4, [208](#)
 - ipv6, [208](#)
 - startElement, [207](#)
 - toXML, [207](#)
 - valid_until, [208](#)
- rpki::left_right::msg, [209](#)
 - pdus, [210](#)
 - serve_top_level, [210](#)
 - version, [210](#)
- rpki::left_right::parent_elt, [213](#)
 - attributes, [216](#)
 - booleans, [216](#)
 - bpki_cms_cert, [216](#)
 - bpki_cms_glue, [216](#)
 - bpki_https_cert, [216](#)
 - bpki_https_glue, [216](#)
 - cas, [214](#)
 - element_name, [216](#)
 - elements, [216](#)
 - query_up_down, [214](#)
 - repository, [215](#)
 - serve_post_save_hook, [215](#)
 - serve_rekey, [215](#)
 - serve_revoke, [215](#)
 - sql_template, [217](#)
- rpki::left_right::report_error_elt, [218](#)
 - attributes, [219](#)
 - element_name, [219](#)
 - error_code, [219](#)
 - from_exception, [219](#)
 - self_id, [220](#)
- rpki::left_right::repository_elt, [222](#)
 - attributes, [224](#)
 - bpki_cms_cert, [224](#)
 - bpki_cms_glue, [225](#)
 - bpki_https_cert, [225](#)
 - bpki_https_glue, [225](#)
 - call_pubd, [223](#)
 - element_name, [225](#)
 - elements, [225](#)
 - object_delete, [223](#)
 - object_write, [224](#)
 - parents, [224](#)
 - publish, [224](#)
 - sql_template, [225](#)
 - uri_to_filename, [224](#)
 - use_pubd, [225](#)
 - withdraw, [224](#)
- rpki::left_right::route_origin_elt, [227](#)
 - as_number, [231](#)
 - attributes, [231](#)
 - booleans, [231](#)
 - ca_detail, [229](#)
 - ca_detail_id, [231](#)
 - cert, [231](#)
 - ee_uri, [229](#)
 - ee_uri_tail, [229](#)
 - element_name, [232](#)
 - generate_roa, [229](#)
 - ipv4, [232](#)
 - ipv6, [232](#)
 - regenerate_roa, [229](#)
 - roa, [232](#)
 - roa_uri, [229](#)
 - serve_post_save_hook, [230](#)
 - sql_delete_hook, [230](#)
 - sql_fetch_hook, [230](#)

- sql_insert_hook, 230
- sql_template, 232
- startElement, 230
- update_roa, 230
- withdraw_roa, 231
- rpki::left_right::sax_handler, 233
 - name, 234
 - pdu, 234
 - version, 234
- rpki::left_right::self_elt, 236
 - attributes, 240
 - booleans, 240
 - bpki_cert, 240
 - bpki_glue, 240
 - bscs, 238
 - children, 238
 - client_poll, 238
 - crl_interval, 240
 - element_name, 240
 - elements, 241
 - parents, 238
 - regen_margin, 241
 - regenerate_crls_and_manifests, 238
 - repositories, 238
 - route_origins, 238
 - self_id, 241
 - serve_fetch_all, 239
 - serve_fetch_one, 239
 - serve_post_save_hook, 239
 - serve_rekey, 239
 - serve_revoke, 239
 - sql_template, 241
 - update_children, 239
 - update_roas, 240
 - use_hsm, 241
- rpki::log
 - debug, 52
 - enable_trace, 52
 - error, 52
 - info, 52
 - init, 51
 - note, 52
 - set_trace, 52
 - trace, 52
 - warn, 52
- rpki::log::logger, 242
 - __call__, 242
 - __init__, 242
 - priority, 243
- rpki::manifest::FileAndHash, 243
 - __init__, 243
 - file, 244
 - hash, 244
- rpki::manifest::FilesAndHashes, 244
 - __init__, 244
- rpki::manifest::Manifest, 245
 - __init__, 245
 - explicitVersion, 246
 - fileHashAlg, 246
 - fileList, 246
 - manifestNumber, 246
 - nextUpdate, 246
 - thisUpdate, 246
 - version, 246
- rpki::oids
 - name2oid, 54
 - oid2name, 54
- rpki::publication
 - obj2elt, 56
- rpki::publication::certificate_elt, 247
 - element_name, 248
 - payload_type, 248
- rpki::publication::client_elt, 250
 - attributes, 252
 - base_uri, 252
 - bpki_cert, 252
 - bpki_glue, 252
 - check_allowed_uri, 251
 - clear_https_ta_cache, 252
 - element_name, 253
 - elements, 253
 - endElement, 251
 - serve_fetch_all, 251
 - serve_fetch_one, 252
 - serve_post_save_hook, 252
 - sql_template, 253
- rpki::publication::cms_msg, 254
 - encoding, 255
 - saxify, 255
 - schema, 255
- rpki::publication::config_elt, 257
 - attributes, 259

- config_id, 259
- element_name, 259
- elements, 259
- fetch, 258
- serve_fetch_one, 258
- serve_set, 259
- sql_template, 260
- startElement, 259
- wired_in_config_id, 260
- rpki::publication::control_elt, 262
 - serve_dispatch, 263
- rpki::publication::crl_elt, 264
 - element_name, 265
 - payload_type, 265
- rpki::publication::manifest_elt, 266
 - element_name, 267
 - payload_type, 267
- rpki::publication::msg, 268
 - pdus, 269
 - serve_top_level, 269
 - version, 269
- rpki::publication::publication_
namespace, 270
 - nsmap, 271
 - xmlns, 271
- rpki::publication::publication_object_elt,
272
 - attributes, 274
 - endElement, 273
 - payload, 274
 - serve_dispatch, 273
 - serve_publish, 273
 - serve_withdraw, 274
 - toXML, 274
 - uri_to_filename, 274
- rpki::publication::report_error_elt, 275
 - attributes, 276
 - element_name, 276
 - error_code, 276
 - from_exception, 276
- rpki::publication::roa_elt, 277
 - element_name, 278
 - payload_type, 278
- rpki::publication::sax_handler, 279
 - name, 280
 - pdu, 280
 - version, 280
- rpki::relaxng
 - left_right, 56
 - publication, 56
 - up_down, 56
- rpki::resource_set
 - _bs2long, 58
 - _long2bs, 58
 - _rsplit, 58
 - inherit_token, 59
 - test1, 58
 - test2, 59
- rpki::resource_set::resource_bag, 281
 - __eq__, 282
 - __init__, 282
 - __ne__, 282
 - __str__, 282
 - asn, 283
 - empty, 282
 - from_rfc3779_tuples, 282
 - intersection, 282
 - oversized, 283
 - undersized, 283
 - union, 283
 - v4, 283
 - v6, 283
 - valid_until, 283
- rpki::resource_set::resource_range, 284
 - __cmp__, 285
 - __init__, 285
 - max, 285
 - min, 285
- rpki::resource_set::resource_range_as,
286
 - __str__, 287
 - datum_type, 287
 - min, 287
 - to_rfc3779_tuple, 287
- rpki::resource_set::resource_range_ip,
288
 - __str__, 289
 - _prefixlen, 289
 - make_prefix, 289
 - to_rfc3779_tuple, 289
- rpki::resource_set::resource_range_ipv4,
290

- datum_type, 291
- rpki::resource_set::resource_range_ipv6, 292
 - datum_type, 293
- rpki::resource_set::resource_set, 294
 - __init__, 295
 - __str__, 295
 - _comm, 296
 - contains, 296
 - difference, 296
 - from_sql, 296
 - inherit, 297
 - intersection, 296
 - issubset, 297
 - issuperset, 297
 - symmetric_difference, 297
 - union, 297
- rpki::resource_set::resource_set_as, 298
 - inherit, 300
 - parse_rfc3779_tuple, 299
 - parse_str, 299
 - range_type, 300
 - to_rfc3779_tuple, 299
- rpki::resource_set::resource_set_ip, 302
 - inherit, 304
 - parse_rfc3779_tuple, 303
 - parse_str, 303
 - to_rfc3779_tuple, 303
- rpki::resource_set::resource_set_ipv4, 305
 - afi, 306
 - range_type, 306
- rpki::resource_set::resource_set_ipv6, 307
 - afi, 308
 - range_type, 308
- rpki::resource_set::roa_prefix, 309
 - __cmp__, 310
 - __init__, 310
 - __str__, 310
 - address, 311
 - max, 310
 - max_prefixlen, 311
 - min, 310
 - prefixlen, 311
 - to_resource_range, 310
 - to_roa_tuple, 311
- rpki::resource_set::roa_prefix_ipv4, 312
 - range_type, 312
- rpki::resource_set::roa_prefix_ipv6, 313
 - range_type, 314
- rpki::resource_set::roa_prefix_set, 314
 - __init__, 315
 - __str__, 315
 - from_sql, 315
 - parse_str, 315
 - to_resource_set, 316
 - to_roa_tuple, 316
- rpki::resource_set::roa_prefix_set_ipv4, 316
 - prefix_type, 317
 - resource_set_type, 317
- rpki::resource_set::roa_prefix_set_ipv6, 318
 - prefix_type, 318
 - resource_set_type, 318
- rpki::roa::ROAIPAddress, 319
 - __init__, 319
 - address, 320
 - maxLength, 320
- rpki::roa::ROAIPAddresses, 320
 - __init__, 320
- rpki::roa::ROAIPAddressFamilies, 321
 - __init__, 321
- rpki::roa::ROAIPAddressFamily, 322
 - __init__, 322
 - addresses, 322
 - addressFamily, 322
- rpki::roa::RouteOriginAttestation, 323
 - __init__, 323
 - asID, 324
 - explicitVersion, 324
 - ipAddrBlocks, 324
 - version, 324
- rpki::rpki_engine::ca_detail_obj, 325
 - activate, 327
 - ca, 327
 - ca_cert_uri, 330
 - ca_id, 330
 - child_certs, 327
 - create, 327
 - crl_uri, 327

- delete, [327](#)
- gctx, [330](#)
- generate_crl, [327](#)
- generate_manifest, [328](#)
- generate_manifest_cert, [328](#)
- issue, [328](#)
- issue_ee, [328](#)
- latest_ca_cert, [330](#)
- latest_crl, [330](#)
- latest_manifest, [330](#)
- latest_manifest_cert, [330](#)
- manifest_private_key_id, [330](#)
- manifest_public_key, [330](#)
- manifest_uri, [328](#)
- private_key_id, [330](#)
- public_key, [330](#)
- revoke, [328](#)
- revoked_certs, [329](#)
- route_origins, [329](#)
- sql_decode, [329](#)
- sql_template, [331](#)
- state, [331](#)
- update, [329](#)
- rpki::rpki_engine::ca_obj, [332](#)
 - ca_details, [333](#)
 - check_for_updates, [333](#)
 - construct_sia_uri, [334](#)
 - create, [334](#)
 - delete, [334](#)
 - fetch_active, [334](#)
 - fetch_deprecated, [334](#)
 - fetch_pending, [335](#)
 - fetch_revoked, [335](#)
 - gctx, [336](#)
 - last_crl_sn, [336](#)
 - last_issued_sn, [336](#)
 - last_manifest_sn, [336](#)
 - next_crl_number, [335](#)
 - next_manifest_number, [335](#)
 - next_serial_number, [335](#)
 - parent, [335](#)
 - parent_id, [336](#)
 - parent_resource_class, [336](#)
 - rekey, [335](#)
 - revoke, [336](#)
 - sia_uri, [336](#)
 - sql_template, [336](#)
- rpki::rpki_engine::child_cert_obj, [338](#)
 - __init__, [339](#)
 - ca_detail, [339](#)
 - ca_detail_id, [340](#)
 - cert, [340](#)
 - child, [339](#)
 - child_id, [341](#)
 - fetch, [339](#)
 - gctx, [341](#)
 - reissue, [340](#)
 - revoke, [340](#)
 - sql_template, [341](#)
 - uri, [340](#)
 - uri_tail, [340](#)
- rpki::rpki_engine::revoked_cert_obj, [342](#)
 - __init__, [343](#)
 - ca_detail, [343](#)
 - ca_detail_id, [344](#)
 - expires, [344](#)
 - gctx, [344](#)
 - revoke, [343](#)
 - revoked, [344](#)
 - serial, [344](#)
 - sql_template, [344](#)
- rpki::rpki_engine::rpkid_context, [345](#)
 - __init__, [346](#)
 - bpki_ta, [347](#)
 - build_https_ta_cache, [346](#)
 - clear_https_ta_cache, [346](#)
 - cronjob_handler, [346](#)
 - https_server_host, [347](#)
 - https_server_port, [347](#)
 - https_ta_cache, [347](#)
 - irbe_cert, [348](#)
 - irdb_cert, [348](#)
 - irdb_query, [346](#)
 - irdb_url, [348](#)
 - left_right_handler, [347](#)
 - publication_kludge_base, [348](#)
 - rpkid_cert, [348](#)
 - rpkid_key, [348](#)
 - sql, [348](#)
 - up_down_handler, [347](#)
- rpki::sql::session, [349](#)
 - __init__, [350](#)

- [_exceptions_enabled, 352](#)
 - [_wrap_execute, 350](#)
 - [assert_pristine, 350](#)
 - [cache, 352](#)
 - [cache_clear, 351](#)
 - [close, 351](#)
 - [connect, 351](#)
 - [cur, 352](#)
 - [database, 352](#)
 - [db, 352](#)
 - [dirty, 352](#)
 - [execute, 351](#)
 - [executemany, 351](#)
 - [fetchall, 351](#)
 - [lastrowid, 351](#)
 - [password, 352](#)
 - [ping, 351](#)
 - [sweep, 351](#)
 - [username, 352](#)
- [rpki::sql::sql_persistent, 353](#)
 - [gctx, 357](#)
 - [sql_debug, 357](#)
 - [sql_decode, 354](#)
 - [sql_delete, 354](#)
 - [sql_delete_hook, 355](#)
 - [sql_deleted, 357](#)
 - [sql_encode, 355](#)
 - [sql_fetch, 355](#)
 - [sql_fetch_all, 355](#)
 - [sql_fetch_hook, 355](#)
 - [sql_fetch_where, 356](#)
 - [sql_fetch_where1, 356](#)
 - [sql_in_db, 358](#)
 - [sql_init, 356](#)
 - [sql_insert_hook, 356](#)
 - [sql_is_dirty, 356](#)
 - [sql_mark_clean, 356](#)
 - [sql_mark_deleted, 357](#)
 - [sql_mark_dirty, 357](#)
 - [sql_store, 357](#)
 - [sql_update_hook, 357](#)
- [rpki::sql::template, 358](#)
 - [__init__, 359](#)
 - [columns, 359](#)
 - [delete, 359](#)
 - [index, 359](#)
 - [insert, 359](#)
 - [map, 359](#)
 - [select, 359](#)
 - [table, 360](#)
 - [update, 360](#)
- [rpki::sundial](#)
 - [now, 62](#)
 - [test, 62](#)
- [rpki::sundial::datetime, 360](#)
 - [__add__, 361](#)
 - [__str__, 361](#)
 - [__sub__, 361](#)
 - [earlier, 362](#)
 - [from_sql, 362](#)
 - [fromASNItuple, 362](#)
 - [fromdatetime, 362](#)
 - [fromGeneralizedTime, 362](#)
 - [fromUTCtime, 362](#)
 - [fromXMLtime, 362](#)
 - [later, 363](#)
 - [PKIX_threshold, 364](#)
 - [to_sql, 363](#)
 - [toASNItuple, 363](#)
 - [toGeneralizedTime, 363](#)
 - [totimestamp, 363](#)
 - [toUTCtime, 363](#)
 - [toXMLtime, 364](#)
- [rpki::sundial::timedelta, 364](#)
 - [convert_to_seconds, 365](#)
 - [parse, 365](#)
 - [regex, 365](#)
- [rpki::up_down](#)
 - [nsmmap, 64](#)
 - [xmlns, 64](#)
- [rpki::up_down::base_elt, 366](#)
 - [check_response, 367](#)
 - [endElement, 367](#)
 - [make_b64elt, 367](#)
 - [make_elt, 367](#)
 - [serve_pdu, 367](#)
 - [startElement, 368](#)
- [rpki::up_down::certificate_elt, 369](#)
 - [cert, 370](#)
 - [cert_url, 370](#)
 - [endElement, 370](#)
 - [req_resource_set_as, 371](#)

- req_resource_set_ipv4, 371
- req_resource_set_ipv6, 371
- startElement, 370
- toXML, 370
- rpki::up_down::class_elt, 372
 - __init__, 373
 - cert_url, 374
 - certs, 374
 - class_name, 374
 - endElement, 373
 - from_resource_bag, 373
 - issuer, 374
 - resource_set_as, 374
 - resource_set_ipv4, 375
 - resource_set_ipv6, 375
 - resource_set_notafter, 375
 - startElement, 374
 - suggested_sia_head, 375
 - to_resource_bag, 374
 - toXML, 374
- rpki::up_down::class_response_syntax, 376
 - __init__, 377
 - classes, 377
 - startElement, 377
 - toXML, 377
- rpki::up_down::cms_msg, 378
 - encoding, 379
 - saxify, 379
 - schema, 379
- rpki::up_down::error_response_pdu, 380
 - __init__, 381
 - check_response, 381
 - codes, 382
 - description, 382
 - endElement, 381
 - exceptions, 382
 - status, 382
 - toXML, 381
- rpki::up_down::issue_pdu, 383
 - class_name, 385
 - endElement, 384
 - pkcs10, 385
 - query, 384
 - req_resource_set_as, 385
 - req_resource_set_ipv4, 385
 - req_resource_set_ipv6, 385
 - serve_pdu, 384
 - startElement, 384
 - toXML, 385
- rpki::up_down::issue_response_pdu, 386
 - check_response, 387
- rpki::up_down::list_pdu, 388
 - query, 389
 - serve_pdu, 389
 - toXML, 389
- rpki::up_down::list_response_pdu, 390
- rpki::up_down::message_pdu, 391
 - __str__, 392
 - make_query, 392
 - name2type, 393
 - payload, 393
 - recipient, 394
 - sender, 394
 - serve_error, 392
 - serve_top_level, 393
 - startElement, 393
 - toXML, 393
 - type, 394
 - type2name, 394
 - version, 394
- rpki::up_down::multi_uri, 395
 - __init__, 395
 - __str__, 395
 - rsync, 395
- rpki::up_down::revoke_pdu, 397
 - class_name, 398
 - get_SKI, 398
 - query, 398
 - serve_pdu, 398
 - ski, 398
- rpki::up_down::revoke_response_pdu, 400
- rpki::up_down::revoke_syntax, 401
 - class_name, 402
 - ski, 402
 - startElement, 402
 - toXML, 402
- rpki::up_down::sax_handler, 404
 - name, 405
 - pdu, 405
 - version, 405

- rpki::x509
 - calculate_SKI, 65
 - POWify_OID, 65
- rpki::x509::CMS_object, 407
 - content, 410
 - debug_cms_certs, 410
 - DER, 410
 - dump_on_verify_failure, 410
 - econtent_oid, 410
 - formats, 411
 - get_content, 409
 - get_DER, 409
 - get_POW, 409
 - other_clear, 411
 - POW, 411
 - print_on_der_error, 411
 - require_crls, 411
 - set_content, 409
 - sign, 409
 - verify, 410
- rpki::x509::CRL, 412
 - DER, 414
 - formats, 414
 - generate, 413
 - get_DER, 413
 - get_POW, 413
 - get_POWpkix, 414
 - getIssuer, 414
 - getNextUpdate, 414
 - getThisUpdate, 414
 - pem_converter, 415
 - POW, 415
 - POWpkix, 415
- rpki::x509::DER_CMS_object, 416
 - content, 417
 - decode, 417
 - encode, 417
- rpki::x509::DER_object, 419
 - __cmp__, 421
 - __init__, 421
 - clear, 421
 - DER, 424
 - dumpasn1, 421
 - empty, 421
 - formats, 424
 - from_sql, 421
 - gAKI, 422
 - get_3779resources, 422
 - get_AIA, 422
 - get_AKI, 422
 - get_Base64, 422
 - get_basicConstraints, 422
 - get_DER, 422
 - get_PEM, 423
 - get_SIA, 423
 - get_SKI, 423
 - gSKI, 423
 - hAKI, 423
 - hSKI, 423
 - is_CA, 424
 - other_clear, 425
 - pem_converter, 425
 - set, 424
 - to_sql, 424
- rpki::x509::PEM_converter, 425
 - __init__, 426
 - b, 427
 - e, 427
 - looks_like_PEM, 426
 - to_DER, 426
 - to_PEM, 426
- rpki::x509::PKCS10, 428
 - check_valid_rpki, 429
 - create, 429
 - create_ca, 429
 - DER, 430
 - formats, 430
 - get_DER, 430
 - get_POWpkix, 430
 - getPublicKey, 430
 - pem_converter, 430
 - POWpkix, 431
- rpki::x509::ROA, 432
 - build, 433
 - content_class, 433
 - econtent_oid, 433
 - pem_converter, 433
- rpki::x509::RSA, 434
 - DER, 437
 - formats, 437
 - generate, 435
 - get_DER, 435

- get_POW, 436
- get_public_DER, 436
- get_RSAPublic, 436
- get_SKI, 436
- get_tlslite, 436
- pem_converter, 437
- POW, 437
- tlslite, 437
- rpki::x509::RSAPublic, 438
 - DER, 440
 - formats, 440
 - get_DER, 439
 - get_POW, 439
 - get_SKI, 439
 - pem_converter, 440
 - POW, 440
- rpki::x509::SignedManifest, 441
 - build, 442
 - content_class, 442
 - econtent_oid, 442
 - getNextUpdate, 442
 - getThisUpdate, 442
 - pem_converter, 443
- rpki::x509::X509, 444
 - DER, 447
 - formats, 447
 - get_DER, 445
 - get_POW, 446
 - get_POWpkix, 446
 - get_tlslite, 446
 - getIssuer, 446
 - getNotAfter, 446
 - getNotBefore, 446
 - getPublicKey, 446
 - getSerial, 447
 - getSubject, 447
 - issue, 447
 - normalize_chain, 447
 - pem_converter, 448
 - POW, 448
 - POWpkix, 448
 - tlslite, 448
- rpki::x509::XML_CMS_object, 450
 - content, 452
 - decode, 451
 - dump_inbound_cms, 452
 - dump_outbound_cms, 453
 - dump_to_disk, 451
 - econtent_oid, 453
 - encode, 451
 - pretty_print_content, 452
 - schema_check, 452
 - unwrap, 452
 - wrap, 452
- rpki::xml_utils::base_elt, 454
 - __str__, 455
 - attributes, 456
 - booleans, 456
 - elements, 457
 - endElement, 455
 - make_b64elt, 455
 - make_elt, 455
 - make_pdu, 455
 - read_attrs, 456
 - startElement, 456
 - toXML, 456
- rpki::xml_utils::data_elt, 458
 - endElement, 459
 - make_reply, 459
 - make_reply_clone_hook, 459
 - serve_create, 459
 - serve_destroy, 460
 - serve_dispatch, 460
 - serve_get, 460
 - serve_list, 460
 - serve_post_save_hook, 460
 - serve_pre_save_hook, 460
 - serve_set, 461
 - toXML, 461
 - unimplemented_control, 461
- rpki::xml_utils::msg, 462
 - __str__, 463
 - endElement, 463
 - startElement, 463
 - toXML, 463
 - type, 463
 - version, 463
- rpki::xml_utils::sax_handler, 465
 - __init__, 466
 - characters, 466
 - create_top_level, 466
 - endElement, 467

- endElementNS, 467
- result, 468
- saxify, 467
- stack, 468
- startElement, 467
- startElementNS, 467
- text, 468
- rpki_checker
 - rpki::https::httpsServer, 183
- rpki_content_type
 - rpki::https, 49
- rpki_engine.py(1873), 484
- rpki_find_handler
 - rpki::https::requestHandler, 184
- rpki_handlers
 - rpki::https::requestHandler, 184
- rpki_issuer
 - rootd, 44
- rpki_key
 - rootd, 44
- rpki_pkcs10_filename
 - rootd, 44
- rpki_server_cert
 - rpki::https::httpsServer, 183
- rpki_server_key
 - rpki::https::httpsServer, 183
- rpki_sessionCache
 - rpki::https::httpsServer, 183
- rpki_subject_filename
 - rootd, 44
- rpki_subject_lifetime
 - rootd, 44
- rpkid, 66
 - cfg_file, 67
 - main, 67
 - profile, 67
- rpkid.py(1880), 484
- rpkid_cert
 - irdbd, 38
 - rpki::rpki_engine::rpkid_context, 348
- rpkid_key
 - rpki::rpki_engine::rpkid_context, 348
- rsync
 - rpki::up_down::multi_uri, 395
- saxify
 - irbe-cli::left_right_cms_msg, 94
 - irbe-cli::publication_cms_msg, 106
 - rootd::cms_msg, 131
 - rpki::left_right::cms_msg, 199
 - rpki::publication::cms_msg, 255
 - rpki::up_down::cms_msg, 379
 - rpki::xml_utils::sax_handler, 467
- schema
 - rpki::left_right::cms_msg, 199
 - rpki::publication::cms_msg, 255
 - rpki::up_down::cms_msg, 379
- schema_check
 - rpki::x509::XML_CMS_object, 452
- select
 - rpki::sql::template, 359
- self
 - rpki::left_right::data_elt, 202
- self_id
 - rpki::left_right::report_error_elt, 220
 - rpki::left_right::self_elt, 241
- sender
 - rpki::up_down::message_pdu, 394
- Sequence, 468
- SequenceOf, 469
- serial
 - cross-certify, 32
 - rpki::rpki_engine::revoked_cert_obj, 344
- serial_file
 - cross-certify, 32
- serve_create
 - rpki::xml_utils::data_elt, 459
- serve_destroy
 - rpki::xml_utils::data_elt, 460
- serve_dispatch
 - rpki::publication::control_elt, 263
 - rpki::publication::publication_object_elt, 273
 - rpki::xml_utils::data_elt, 460
- serve_error
 - rpki::up_down::message_pdu, 392
- serve_fetch_all
 - rpki::left_right::data_elt, 202
 - rpki::left_right::self_elt, 239
 - rpki::publication::client_elt, 251

- serve_fetch_one
 - rpki::left_right::data_elt, 202
 - rpki::left_right::self_elt, 239
 - rpki::publication::client_elt, 252
 - rpki::publication::config_elt, 258
- serve_get
 - rpki::xml_utils::data_elt, 460
- serve_list
 - rpki::xml_utils::data_elt, 460
- serve_pdu
 - rootd::issue_pdu, 133
 - rootd::list_pdu, 135
 - rootd::revoke_pdu, 139
 - rpki::up_down::base_elt, 367
 - rpki::up_down::issue_pdu, 384
 - rpki::up_down::list_pdu, 389
 - rpki::up_down::revoke_pdu, 398
- serve_post_save_hook
 - rpki::left_right::child_elt, 196
 - rpki::left_right::parent_elt, 215
 - rpki::left_right::route_origin_elt, 230
 - rpki::left_right::self_elt, 239
 - rpki::publication::client_elt, 252
 - rpki::xml_utils::data_elt, 460
- serve_pre_save_hook
 - rpki::left_right::bsc_elt, 191
 - rpki::xml_utils::data_elt, 460
- serve_publish
 - rpki::publication::publication_object_elt, 273
- serve_rekey
 - rpki::left_right::parent_elt, 215
 - rpki::left_right::self_elt, 239
- serve_revoke
 - rpki::left_right::parent_elt, 215
 - rpki::left_right::self_elt, 239
- serve_set
 - rpki::publication::config_elt, 259
 - rpki::xml_utils::data_elt, 461
- serve_top_level
 - rpki::left_right::msg, 210
 - rpki::publication::msg, 269
 - rpki::up_down::message_pdu, 393
- serve_up_down
 - rpki::left_right::child_elt, 196
- serve_withdraw
 - rpki::publication::publication_object_elt, 274
- server
 - rpki::https, 48
- server_cert
 - irdbd, 38
 - rootd, 44
- server_ta
 - irbe-cli, 35
- set
 - rpki::x509::DER_object, 424
- set_content
 - rpki::x509::CMS_object, 409
- set_subject_cert
 - rootd, 42
- set_trace
 - rpki::log, 52
- sia_uri
 - rpki::rpki_engine::ca_obj, 336
- sign
 - rpki::x509::CMS_object, 409
- signing_cert
 - irbe-cli::bsc_elt, 73
 - rpki::left_right::bsc_elt, 192
- signing_cert_crl
 - irbe-cli::bsc_elt, 73
 - rpki::left_right::bsc_elt, 192
- ski
 - rpki::up_down::revoke_pdu, 398
 - rpki::up_down::revoke_syntax, 402
- sql
 - pubd::pubd_context, 128
 - rpki::rpki_engine::rpkid_context, 348
- sql.py(1873), 484
- sql_debug
 - rpki::sql::sql_persistent, 357
- sql_decode
 - rpki::rpki_engine::ca_detail_obj, 329
 - rpki::sql::sql_persistent, 354
- sql_delete
 - rpki::sql::sql_persistent, 354
- sql_delete_hook

- rpki::left_right::route_origin_elt, 230
- rpki::sql::sql_persistent, 355
- sql_deleted
 - rpki::sql::sql_persistent, 357
- sql_encode
 - rpki::sql::sql_persistent, 355
- sql_fetch
 - rpki::sql::sql_persistent, 355
- sql_fetch_all
 - rpki::sql::sql_persistent, 355
- sql_fetch_hook
 - rpki::left_right::route_origin_elt, 230
 - rpki::sql::sql_persistent, 355
- sql_fetch_where
 - rpki::sql::sql_persistent, 356
- sql_fetch_where1
 - rpki::sql::sql_persistent, 356
- sql_in_db
 - rpki::sql::sql_persistent, 358
- sql_init
 - rpki::sql::sql_persistent, 356
- sql_insert_hook
 - rpki::left_right::route_origin_elt, 230
 - rpki::sql::sql_persistent, 356
- sql_is_dirty
 - rpki::sql::sql_persistent, 356
- sql_mark_clean
 - rpki::sql::sql_persistent, 356
- sql_mark_deleted
 - rpki::sql::sql_persistent, 357
- sql_mark_dirty
 - rpki::sql::sql_persistent, 357
- sql_store
 - rpki::sql::sql_persistent, 357
- sql_template
 - rpki::left_right::bsc_elt, 192
 - rpki::left_right::child_elt, 197
 - rpki::left_right::parent_elt, 217
 - rpki::left_right::repository_elt, 225
 - rpki::left_right::route_origin_elt, 232
 - rpki::left_right::self_elt, 241
 - rpki::publication::client_elt, 253
 - rpki::publication::config_elt, 260
 - rpki::rpki_engine::ca_detail_obj, 331
 - rpki::rpki_engine::ca_obj, 336
 - rpki::rpki_engine::child_cert_obj, 341
 - rpki::rpki_engine::revoked_cert_obj, 344
- sql_update_hook
 - rpki::sql::sql_persistent, 357
- stack
 - rpki::xml_utils::sax_handler, 468
- startElement
 - rpki::left_right::list_resources_elt, 207
 - rpki::left_right::route_origin_elt, 230
 - rpki::publication::config_elt, 259
 - rpki::up_down::base_elt, 368
 - rpki::up_down::certificate_elt, 370
 - rpki::up_down::class_elt, 374
 - rpki::up_down::class_response_-syntax, 377
 - rpki::up_down::issue_pdu, 384
 - rpki::up_down::message_pdu, 393
 - rpki::up_down::revoke_syntax, 402
 - rpki::xml_utils::base_elt, 456
 - rpki::xml_utils::msg, 463
 - rpki::xml_utils::sax_handler, 467
- startElementNS
 - rpki::xml_utils::sax_handler, 467
- startup_msg
 - irdbd, 38
- stash_subject_pkcs10
 - rootd, 42
- state
 - rpki::rpki_engine::ca_detail_obj, 331
- status
 - rpki::up_down::error_response_pdu, 382
- suggested_sia_head
 - rpki::up_down::class_elt, 375
- sundial.py(1873), 485
- sweep
 - rpki::sql::session, 351

- symmetric_difference
 - rpki::resource_set::resource_set, 297
- table
 - rpki::sql::template, 360
- test
 - rpki::sundial, 62
- test1
 - rpki::resource_set, 58
- test2
 - rpki::resource_set, 59
- text
 - rpki::xml_utils::sax_handler, 468
- textwrap::TextWrapper, 469
- thisUpdate
 - rpki::manifest::Manifest, 246
- tlslite
 - rpki::x509::RSA, 437
 - rpki::x509::X509, 448
- tlslite::api::Checker, 470
- tlslite::api::HTTPTLSConnection, 470
- tlslite::api::TLSSocketServerMixIn, 471
- tlslite_certChain
 - rpki::https, 48
- to_DER
 - rpki::x509::PEM_converter, 426
- to_PEM
 - rpki::x509::PEM_converter, 426
- to_resource_bag
 - rpki::up_down::class_elt, 374
- to_resource_range
 - rpki::resource_set::roa_prefix, 310
- to_resource_set
 - rpki::resource_set::roa_prefix_set, 316
- to_rfc3779_tuple
 - rpki::resource_set::resource_range_as, 287
 - rpki::resource_set::resource_range_ip, 289
 - rpki::resource_set::resource_set_as, 299
 - rpki::resource_set::resource_set_ip, 303
- to_roa_tuple
 - rpki::resource_set::roa_prefix, 311
- rpki::resource_set::roa_prefix_set, 316
- to_sql
 - rpki::sundial::datetime, 363
 - rpki::x509::DER_object, 424
- toASN1tuple
 - rpki::sundial::datetime, 363
- toGeneralizedTime
 - rpki::sundial::datetime, 363
- top_opts
 - irbe-cli, 35
- totimestamp
 - rpki::sundial::datetime, 363
- toUTCTime
 - rpki::sundial::datetime, 363
- toXML
 - rpki::left_right::list_resources_elt, 207
 - rpki::publication::publication_object_elt, 274
 - rpki::up_down::certificate_elt, 370
 - rpki::up_down::class_elt, 374
 - rpki::up_down::class_response_syntax, 377
 - rpki::up_down::error_response_pdu, 381
 - rpki::up_down::issue_pdu, 385
 - rpki::up_down::list_pdu, 389
 - rpki::up_down::message_pdu, 393
 - rpki::up_down::revoke_syntax, 402
 - rpki::xml_utils::base_elt, 456
 - rpki::xml_utils::data_elt, 461
 - rpki::xml_utils::msg, 463
- toXMLtime
 - rpki::sundial::datetime, 364
- trace
 - rpki::log, 52
- type
 - rpki::up_down::message_pdu, 394
 - rpki::xml_utils::msg, 463
- type2name
 - rootd::message_pdu, 137
 - rpki::up_down::message_pdu, 394
- u
 - irdbd, 39

- undersized
 - rpki::resource_set::resource_bag, 283
- unimplemented_control
 - rpki::left_right::data_elt, 203
 - rpki::xml_utils::data_elt, 461
- union
 - rpki::resource_set::resource_bag, 283
 - rpki::resource_set::resource_set, 297
- unwrap
 - rpki::x509::XML_CMS_object, 452
- up_down
 - rpki::relaxng, 56
- up_down.py(1873), 485
- up_down_handler
 - rootd, 42
 - rpki::rpki_engine::rpkid_context, 347
- update
 - rpki::rpki_engine::ca_detail_obj, 329
 - rpki::sql::template, 360
- update_children
 - rpki::left_right::self_elt, 239
- update_roa
 - rpki::left_right::route_origin_elt, 230
- update_roas
 - rpki::left_right::self_elt, 240
- uri
 - rpki::rpki_engine::child_cert_obj, 340
- uri_tail
 - rpki::rpki_engine::child_cert_obj, 340
- uri_to_filename
 - rpki::left_right::repository_elt, 224
 - rpki::publication::publication_object_elt, 274
- url
 - irbe-cli, 36
- usage
 - cross-certify, 31
 - irbe-cli, 34
 - irbe-cli::cmd_elt_mixin, 84
 - irbe-cli::cmd_msg_mixin, 86
- usage_fill
 - irbe-cli, 36
- use_hsm
 - rpki::left_right::self_elt, 241
- use_pubd
 - rpki::left_right::repository_elt, 225
- username
 - rpki::sql::session, 352
- v4
 - rpki::resource_set::resource_bag, 283
- v6
 - rpki::resource_set::resource_bag, 283
- valid_until
 - rpki::left_right::list_resources_elt, 208
 - rpki::resource_set::resource_bag, 283
- verbose
 - irbe-cli, 36
- verify
 - rpki::x509::CMS_object, 410
- version
 - rpki::left_right::msg, 210
 - rpki::left_right::sax_handler, 234
 - rpki::manifest::Manifest, 246
 - rpki::publication::msg, 269
 - rpki::publication::sax_handler, 280
 - rpki::roa::RouteOriginAttestation, 324
 - rpki::up_down::message_pdu, 394
 - rpki::up_down::sax_handler, 405
 - rpki::xml_utils::msg, 463
- warn
 - rpki::log, 52
- wired_in_config_id
 - rpki::publication::config_elt, 260
- withdraw
 - rpki::left_right::repository_elt, 224
- withdraw_roa
 - rpki::left_right::route_origin_elt, 231

- wrap
 - rpki::x509::XML_CMS_object, [452](#)
- x
 - cross-certify, [32](#)
- x509.py(1873), [486](#)
- x509store
 - rpki::https::Checker, [180](#)
- x509store_thunk
 - rpki::https::Checker, [179](#)
- xml::sax::handler::ContentHandler, [472](#)
- xml_utils.py(1873), [486](#)
- xmlns
 - rpki::left_right::left_right_namespace, [205](#)
 - rpki::publication::publication_namespace, [271](#)
 - rpki::up_down, [64](#)