PKI REST API Documentation

PKI provides a REST interface mode. This API allows to:

- Request a certificate (and issue it in PKCS12 format)
- Revoke a certificate
- Search for a certificate
- Issue the CRL
- List the certificate profiles

All parameters must be passed as UTF-8 (URL encoded depending on the HTTP GET/POST method used).

Requesting a certificate

To request a certificate, following HTTP request should be performed:
wget --user=admin --password=<pki_admin_password> "https://<pki_host>/pki/?action=enroll&cn=Test&email=test@example.org&pwd=test&crt_type=auth_cert&direct=1"

Note that this is explained using wget and GET HTTP parameters for the sake of simplicity, but HTTP POST requests can be performed instead, with the following request parameters:

- cn: requested certificate CN
- email: requested certificate email address (or MSUPN for the SmartCard Logon profile)
- pwd: password used to encrypt the certificate and its key (PKCS#12)
- crt_type: type of requested certificate (normally auth_cert)
- direct: 1 (to activate REST mode)
- action: enroll (to request a certificate)

This request returns an application/json reply, containing a JSON message with either "OK" and a Base64 encoded pkcs12, or an error message in case of error.

Note
It is possible to enroll in decentralized mode as well, with the following modifications:

- action: enroll_pkcs10
- pkcs10: the Certificate Sign Request, in PKCS10 format
- pwd: should not be mentioned
- lifetime: life time of the certificate (optional, if not present certificate profile setting is used)
- device_sn: serial number of the device on which is hosted the private key of the certificate (optional)

In this case, the certificate is returned as PEM-encoded PKCS7 X509v3.

Revoking a certificate

To revoke a certificate, following HTTP request should be performed:
wget --user=admin --password=<pki_admin_password> "https://<pki_host>/pki/?action=revoke&rev_serial=<cert_serial_number>&direct=1"

Note that this is explained using wget and GET HTTP parameters for the sake of simplicity, but HTTP POST requests can be performed instead, with the following request parameters:

- rev_serial: serial number of the certificate to revoke
- direct: 1 (to activate REST mode)
- action: revoke (to revoke a certificate)

This request returns an application/json reply, containing a JSON message with either "OK" or an error message in case of error.
WARNING: in JSON mode, the CRL is NOT issued upon revocation.

Searching for certificates

To search for a certificate, following HTTP request should be performed:
wget --user=admin --password=<pki_admin_password> "https://<pki_host>/pki/?action=search&search_dn=<dn_part_to_search>&direct=1

Note that this is explained using wget and GET HTTP parameters for the sake of simplicity, but HTTP POST requests can be performed instead,
with the following request parameters:

- search_dn: dn or part of dn to search for (substring match)
- search_profile: certificate profile used to issue the certificate (optional)
- action: search
- direct: 1 (to activate REST mode)

Each result line has the following structure:
"STATUS,SERIAL,EXPIRATION_DATE,REVOCATION_DATE,SUBJECT_DN"

Example response to search call:

```
{
"status" : "OK",
"count" : "2",
"res0" : "V,2156EFD0BEA0,161120095128Z,,/C=FR/O=MyDev/OU=Server/
CN=Alcide Loopkin/email=loopkin@nikosoft.net",
"res1" : "V,213713C9EF5D,161115210452Z,,/C=FR/O=MyDev/OU=Server/
CN=Alcidette Loopkin/email=loopkin@nikosoft.net"
}
```

Retrieving a certificate

To retrieve a certificate, following HTTP request should be performed:
wget --user=admin --password=<pki_admin_password> "https://<pki_host>/pki/?action=viewcert&view_serial=<serial_of_cert_to_retrieve>&direct=1

Note that this is explained using wget and GET HTTP parameters for the sake of simplicity, but HTTP POST requests can be performed instead,
with the following request parameters:

- view_serial: serial number of the certificate to retrieve
- action: viewcert
- direct: 1 (to activate REST mode)

Issuing CRL

To issue a CRL, following HTTP request should be performed:
wget --user=admin --password=<pki_admin_password> "https://<pki_host>/pki/?action=crlgen&direct=1"

This request returns an application/json reply, containing a JSON message with either "OK" or an error message in case of error.

Listing certificate profiles

To list the available certificate profiles, following HTTP request should be performed:
wget --user=admin --password=<pki_admin_password> "https://<pki_host>/pki/?action=list_profiles&direct=1"

This request returns an application/json reply, containing a JSON message with either "OK" and the list of certificate profiles, or an error message in case of error.

Example response to the list_profiles call:

```
{
"status" : "OK",
"count" : "4",
"profile0" : "auth_cert",
"profile1" : "dc_cert",
"profile2" : "scl_cert",
"profile3" : "serv_cert"
}
```

Copyright (c) 2014-2015 Alexandre Aufrere - http://ReTrust.me. All Rights Reserved.