PKI Quickstart Guide

Installation

When installing, you need internet access to download extra packages.

1. Install Centos 6 64 bits from "minimal" ISO, or CentOS 7 from "minimal" ISO
2. Execute ./retrustme-pki-install and follow the onscreen instructions
3. Go to the web interface, and generate the CA ("Key Ceremony")
4. Reboot, to ensure all services are started correctly

Optionally, you can use Gemalto-SafeNet HSMs (ProtectServer or Luna). Please refer to additional documentation accordingly.

Note: It supports password authentication OR certificate based authentication.
In case of certificate based authentication, an initial administrator PKCS#12 certificate is created:

- Its password is "retrust123"
- It should be used only to configure the application, and issue the first administrator PKCS#12. Afterwards it MUST be revoked using the "Operators Certificates" menu, after issuing at least one new administrator certificate.

Features

The PKI has the following features:

- REST connector (read the MANUAL.REST file)
- CRMP connector
- Management of one CA, including the Key Ceremony, and periodic CRL generation (once a day)
- Capability to generate and store CA key in hardware modules (eToken,...)
- Issuance of certificate expiration notices one month before expiration
- Issuance of certificates in PKCS12 format (Web interface and REST)
- Issuance of certificates in PKCS7 format from PKCS10 (Web Interface and REST)
- Issuance of certificates on smart card (Web Interface, Internet Explorer 10+ and Minidriver-enabled Smart Card only)
- Search for certificates (Web interface and REST)
- Certificate revocation (Web interface and REST)
- Everything you will find in the Settings, including management of multiple profiles
- Multiple operators support (see bin/manageuser.pl script)
- Backup and restore scripts
- Audit log system, through syslog (see /var/log/nspki.log), and "|" separated files which is signed in SMIME
- Easy usage: by default, everything is configured as needed for typical basic usage

- TimeStamp Authority - RFC 3161
- Ability to configure DN components automatically from email, or statically (gmail.com => DC=gmail, DC=COM; free.fr => O=free, C=FR)
- Issuance of ICAO 9303 MRTD compliant DG and SOD
- Configuration of several items per profile (lifetime, maximum number of users,
- Full control over one custom profile, set in etc/custom_profile.cnf (advanced users)

Tips

Following quick tips can help you:

- If CRL expired for some reason, you can force its re-generation by launching as root: /opt/nspki/bin/cronjob.pl --daily
- To do a Key Ceremony using an external root CA, do it first using the internal workflow, then download CA CSR from "CA Management" menu, and import back the CA certificate using the /opt/nspki/bin/installcacert.pl script
- Launching the scripts in /opt/nspki/bin with "--help" will give you more information about each of them
- The product manages the DB itself, including the laundry. No need to take care of it.
- Quick help is available in most places of the product, by just hovering over the fields.
- A lifetime of "0" (certificate templates) means actually 1 hour (useful for OTF certificates)
- If you install using VirtualBox, please create 2 interfaces: one NAT (for internet access), and one Host-only networking (so that you can access from the host)

List of man pages

MANUAL
MANUAL.MRTD
MANUAL.PROTECTSERVER
MANUAL.REST
MANUAL.SCEP
MANUAL.SMARTCARDLOGON
MANUAL.tmp