Plug and Play CA -Quick start...

Certification Authority which just works

Aleksander Nowiński

Introduction

Welcome to Plug-and-Play Certification Authority quickstart document. This document will help you to run a PnP CA service within less than 5 minutes.

Install service

Select location for your CA server (usually /opt will be ok on linux systems) and unpack there installation package (zip or tar.gz, content is exactly the same). This is all.

Ensure your system has installed Java 6 (best in SUN version, but shall not be a problem to use OpenJDK). Ensure you have Unlimited Strength Cryptography policy files installed. If not, install it now.

Update initial configuration

For sure you shall update following parts of `conf/config.xml` file before first run:

- `web/title` – this is name of your CA as it will be used on web pages and in emails
- `ca/localDN` – dn of certificate which will be generated for CA on startup. If you start before changing it, to generate new certificate delete local/keystore.p12 and local/cert.pem

Later on, you shall definitely update:

- `web/http, web/https` – ports and protocols service will use. Defaults are reasonable.
- `web/admin` – CA administrator contact information
- `mail/*` - you email notification settings

And for sure update `loca/userMap` to set your username and password and remove default ones. Syntax is: user=password, role (required role is admin). Instead of plaintext password you may use MD5 sum of password, with MD5:<sum value> instead of password.

Start the server

To start the server invoke `bin/pnpca` script. On windows you may run:

```
java -jar pnpca-<version>.jar
```

in main server directory.

Test installation

To see whether your installation is OK connect with your browser to address http://localhost:8080/

If you will see your CA main page, then you have succeeded. You may now submit

Troubleshooting

To see what is problem with server you shall examine server logs. There are two log files interesting for you:

`logs/startup.log` – file containing java startup information. If something appears there, then there is probably a problem with paths, libraries of java installation

`logs/pnpca.log` – file with server log from operation. Examine it if server fails to start –

probably there is a problem with Unlimited Strength Cryptography policy or with configuration files

Also after failed startup ensure that file `local/keystore.p12` is not empty. If it is use `bin/clear_ca` script (or remove `local/keystore.p12` and `local/cert.pem` manually).

And now...

PnP CA is ready to use. Now, to update your configuration install properly permissions and make it run on server boot you shall consult main manual, which is way more informative.