AustrianGrid CA:Update

Certification Authority

Willy Weisz

EUGridPMA Meeting, Poznan
8 September 2014

Why the change?

Improve turn-around for subscriber requests

- Reduce manual intervention for signing certificates and CRL
- Setup online CA with HSM
- Empower RA bypassing CA intervention whenever possible

Why now?

AustrianGrid CA certificate is about to expire (10 March 2015)

New and re-keyed certificates issued with validity until 10 March 2015

Programming of user interface progressed slowly with longer interruptions

- Lately gained momentum

Architecture

2 CAs

- Root CA on off-line server
  - Probable move to Raspberry Pi
- End-entity CA
  - Online server with world wide access to local web server
  - and with a second network connection with IPv4 private addresses to
  - Signing server with HSM (Safenet ProtectServer Gold) – FIPS 140-2 level 3

Root CA

Offline whenever the private key is available (even when encrypted)

- RSA keys with 4096 bit module
- Each CA staff has a copy of the private key encrypted with a passphrase of 12+ characters that only he/she knows
- Encrypted copy of private key on non over-writable removable medium – passphrase in sealed envelop separate from storage medium
- Certificate valid 20 years
- CRLs valid 13 months, re-issued after one year

IGTF Classic end-entity CA

2 servers

One front-end server

- Repository
- Web server for key pair/CSR generation on the system of the subscriber (through an applet in the web browser)
- Storage for CSRs to be processed
- RA browser interface for processing requests
- Web server for certificate delivery to subscriber
- Web server for revocation requests by subscribers possessing the private key

Front-end server

Enrollment for person certificates:

- Subscriber without certified key pair
  - Inputs personal data
  - Generates key pair/CSR with parameters compatible with „Grid Certificate Profile“ (GWD-R 125bis)
  - CSR sent to server
  - RA waits for face-to-face meeting before releasing CSR for certificate signing

Front-end server

- Subscriber with certified key pair to re-key
  - Authenticates to web server via browser
  - Generates key pair/CSR with parameters compatible with „Grid Certificate Profile“ (GWD-R 125bis)
  - CSR sent to server
  - RA can release CSR for certificate signing without delay

Front-end server

Server/service certificate

- Institution defines who can request server/service certificate for own domain
- When these persons authenticate to the web server, they can choose to request server/service certificates (or re-keys thereof)
- RA can release request for certificate issuance without delay
- Same persons can also request revocation of server/service certificates for their domain

Back-end server

Front-end server communicates via 2nd network interface card with back-end over IPv4 private address space

Back-end has HSM (Safenet ProtectServer Gold) compliant with FIPS 140-2 level 3.

Key pair with 4096 bit module

Script

- fetches CSR from NFS server on front-end
- generates the certificate and the signature hash (SHA512)
- feeds the hash to the HSM for encryption with the private key
- stores the certificate on NFS share on front-end

Back-end server

CRL generation is requested on front-end

Request leaves a file with the certificate serial to revoke on NFS share on front-end

Script on backend

- fetches request, initiates CRL generation and signing
- returns CRL to NFS share on front-end

CRL is moved to repository

End-entity certificates

RSA keys

Size: 2048 bit module or more (in 1024 bit increments)

alternativeSubjectNames:

1 or more e-mail addresses for person certificates

1 or more DNS addresses for server/service certs

Choice among optional keyUsages according to GWD-R 125bis

End-entity certificates

Certificate issuance is communicated to subscriber via e-mail containing a web address

Call of that web address initiates a browser application (applet) that creates a PKCS#12 file storing the certificate and the private key that is to be found at the file system location it was created – the ability to create that file is second proof of private-key ownership as well as „conduct constituting certificate acceptance“

End-entity certificates

SubjectNames:

DC=at, DC=austriangridca, O=*organisation,* OU=...,CN=*person-name or FQDN*

Subscribers with subjectNames from „old“ AustrianGrid CA

C=AT, O=Austrian Grid, OU=*organisation*, …

may retain old subjectName, even so automatic move to new address space is recommended

Some questions

- CP/CPS OID not in policies entry of CA certificates?
- Must the activation password for the HSM entered at the start of operation, or can it reside in a configuartion file, well protected by the O/S?