KFKI CA

József Kadlecsik
KFKI RMKI
kadlec@sunserv.kfki.hu

The KFKI Campus

- Hosts five independent academic research institutes
- One of them is the KFKI Research Institute for Particle and Nuclear Physics (KFKI RMKI)
- The Computer Networking Center of KFKI RMKI is responsible for the central computing and network services of the KFKI Campus

KFKI CA

- No subordinate CAs
- One RA, which is performed by the KFKI CA itself
- No plan for additional RAs
- Usual defaults:
  - Root CA key: 5 years, 2048 bits
  - Entity keys: 1 year, min 1024 bits
  - CRLs: after revocation or every month

KFKI CA end entities I.

- Academic entities of the KFKI Campus:
  - Institutions
  - Individuals, computers, services belonging to the institutions
  - External individuals involved in the scientific, research projects of the academic institutions

  Cert usages: user/host certs for Grid, service certs (http, pop/imap, smtp), user certs for roaming users (smtp ssl/tls)

KFKI CA end entities II.

- Entities of the Hungarian academic community involved in Grid related scientific or research projects.

Authentication of organizations

- Campus organization: RA directly contacts the representative for the autheticity of the request
- Non-campus organization: official document stamped and signed by the official representative of the organization is required

Authentication of individuals

- Local requester must appear in-person before the RA and show the identification card, passport or driving licence
- If the RA personally knows the requester, authentication over phone call is accepted
- Distant subscriber: copy of the identity card manually signed by a well-known contact person of the organization required and the subscriber is called back on the official phone number for further checkings.

Authentication of machine/service

- Either the requester must fulfil the individual authentication, or the request must be signed by the requester's valid cert issued by KFKI CA
- Requester must adequately prove that he/she is responsible for the entity in question: checked by the computer technical contact persons of the institutions

Re-keying

- The request must contain a new public key
- Authentication is either as a new request, or request must be signed by the valid non-expired, non-revoked certificate of the requester

Namespace

- Fixed part: C=HU,O=KFKI
- C=HU,O=KFKI,OU=people,CN=Kiss Istvan
- C=HU,O=KFKI,OU=services,CN=www.kfki.hu
- C=HU,O=KFKI,OU=services,
  CN=ldap/ldap.kfki.hu
- C=HU,O=KFKI,OU=grid,OU=people,
  CN=Kiss Pal

Hungarian ISO Latin 2 chars are converted:

é -> e, í -> i, ó -> o, ő -> o, ...

Technical details

- Dedicated Linux PCs with CD writer drive
  - Full system backup on CD
- Signing machine has no network card, locked in a room on the first floor of the building of the Computer Networking Center
- Removable media is kept in a secure cabinet, backups in multiple locations

Software

- OpenCA
- Sleepycat DB
- Apache
- RBAC not activated yet - we are more accustomed to LIDS

Open issues

- Requests sent by E-mail (S/MIME) should be imported into OpenCA
- User interface for re-keying
- Full Hungarian translation of the user interface

Suggestions are welcomed!