NIIF CA status

Tamás Máray
NIIF/Hungarnet

EUGridPMA meeting, Jan. 2013, Rome

General information

- NIIF CA is an X.509 PKI CA with *online* CA infrastructure
- Hardware: two computers (SunFire 120 + a regular 1U Intel based server) and a hardware security module (HSM): Chrysalis Luna crypto HW (FIPS140-2 Level 3) + a mgmt workstation
- Software: Solaris, Linux and Sun Certificate Management System (CMS)
- Root CERT: 2048 bit long, 10 years lifetime (expires in 2015)

General information

- The NIIF CA was accredited by EUGridPMA in 2005 January
- It provides free X.509 grid and non-grid user and host certificates for the academic user community (research and higher education)
- Located in Budapest in a safe machine room, operated by NIIF Institute (the Hungarian NREN)
- Very stable and smooth operation

NIIF CA status

- As of yesterday:
  - 1351 CERTs are issued in total
  - 149 CERTs are valid
    - 131 grid, 18 other
  - 1149 CERTs are expired
  - 53 CERTs are revoked

- About 15% of all the CERTs are for hosts, 85% for users

Additional remark

- NIIF is a member of the TERENA TCS community, currently offering only TCS server certs for its customers
  - 1552 certs are issued
  - 1031 are valid
- No eScience server certificates issued yet

Self audit of the CA

- Last self audit of the NIIF CA was performed in 2009
- No critical issues found, but a number of things to be corrected/improved
- Most of them are done, and modified CP/CPS were published accordingly
- However: some issues are still not fixed:
  - Restructuring the CP/CPS documents according to RFC3647
  - Inclusion of FQDN in the SubjectAlternativeName of server CERTs
  - Preparation of Operation Manual and Disaster Recovery Plan documents
- The next self audit should have been performed last year… Apologies and reasons…

The future of the NIIF CA

The future of the NIIF CA

?

Problems

- Part of the HW is old and not supported anymore
- Part of the SW is old and not supported anymore
- Cost of operation is relatively high
- Root CERT will expire soon in 2015
- User demands for grid CERTs is very limited and won’t grow

Solution no.1

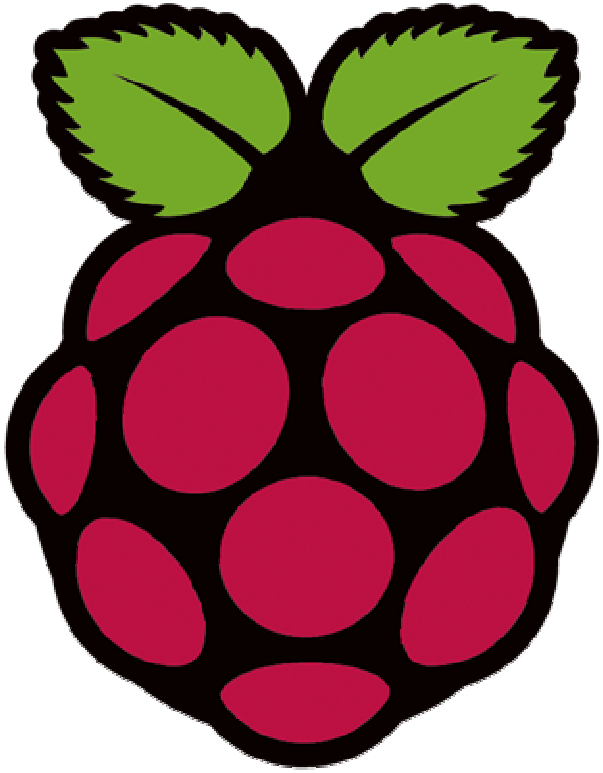
- Migrate to TERENA TCS eScience certificates
  - (btw: very expensive, if you only have a small number of certs)

- Shut down the NIIF CA according to the rules described in the CP (timely process)

Solution no.2

- Renew the NIIF CA infrastructure (HW + SW)

- We have got an idea…



Building a CA with Raspberry PI

- A tiny (credit card size) very cheap, very power efficient “single chip” computer running Linux

with USB crypto HW

- eg. LOK-IT or similar

The new CA

- Two Raspberry PIs + an USB crypto HW
- On-line CA, architecturally similar to the old one
- Open source, customized CA SW, like OpenCA
- Going GREEN! 150 times less energy consumption and CO2 footprint!
- Do you know, how many tons(!) of CO2 is generated by your CA yearly?

Protecting the environment

- At NIIF CA currently each and every grid CERT pollutes the atmosphere with ~14kg of greenhouse gas /year!
- With this new solution we can go down to 90 gr/cert/year

- The yearly energy cost of the CA will also drop from ~800 euro to ~5 euro!

But

No decision is made yet..

Pros and cons are currently evaluated

Thank you!