
# SiGNET CA Report and Self-Assessment

Jan Jona Javoršek, Borut Paul Kerševan
jan.javorsek@ijs.si borut.kersevan@ijs.si

SiGNET CA
Jozef Stefan Institute
Slovenia

signet-ca@ijs.si

EU Grid PMA, Copenhagen, 28th May 2008

# Current Status

- 2004-2008, SiGNET CA is still a small CA
  - 1 RA (at the CA)
  - ~ 50 valid certificates
  - > 80 % host and service certificates
- But we seem to be getting bigger
  - new institutions requesting certificates
  - founding to the NGI
  - NGI will have a new RA

# Operational setup

SiGNET CA

- Heavily patched OpenCA
  - based on 0.9.2
  - local quick set-up scripts
  - database export scripts
  - backup scripts
- An offline CA
- Only software tokens issued so far

# Recent events

SiGNET CA

- Hot disaster recovery tests
  - survived a complete hw failure on online machine
    - quick install and db restore worked flawlessly
    - now keeping a failback in a VM
  - hard drive failure on offline machine
    - lost only logs from last successful login
    - rebuild a new set-up from backup
    - improved backup procedures

# Other Operational Notes


- Still occasionally behind with CRL
  - (i.e. 5 days before end of life)
  - In spite of two Nagios checking services!
  - Solution: improved procedures for the present CA administrator
- IGTF Nagios monitoring service behind repository releases
  - developed automatic monitor update

# Self-Assessment


- Self-Assessment based on Guidelines for Auditing CAs by Yoshio Tanaka and Mathew Viljoen
- Done in parallel with:
  - CP/CPS update
  - transfer of CP/CPS to RFC 3647 form
  - consideration of some technical difficulties
  - plans for the future

# Problems Found

SiGNET CA

- Several updates to conform to IGTF-AP Classic Profile version 4.1:
  - CP/CPS was re-structured according to RFC 3647
  - Added missing provision for RA to respond in 3 working days
  - Added requirement for operational audits of personnel and maintenance of personnel lists
  - Added requirement for subscriber's key backups

# Problems found

SiGNET CA

- ...
  - Added requirement for yearly self-assessment
  - Fixed missing subjectAlternativeName fields and Netscape Object signing extensions
    - both existed in practice [A!]
  - CRL version number changed to v2 in CP/CPS
    - matching practice [A!]

# Improvements in CP/CPS

SiGNET CA

- Description of what constitutes certificate acceptance (after retrieval, subscriber has 5 working days to refuse the certificate)
- Clarification on what kind of changes to CP/CPS require OID change
- A number of clarifications
- Nitpicks

# New Provisions

SiGNET CA

- Allowance for FQDN in subjectAlternativeName
- Provisions for an OCSP service
- Dropped non-repudiation

# Future plans

SiGNET CA

- Getting bigger
  - working with ARNES to set up a chain of NGI RAs for the CA
- A new set-up
  - with a HSM
- A MICS profile
  - for the institute or larger
- ... regular updates and self-assessments

# Questions?

Draft version of SiGNET CA/CPS v1.1 for the impatient:

http://www-f9.ijs.si/~jona/cpcps/signet_ca-cps_v1.1.html