INFN CA Internal Audit

Roberto Cecchini

XIV EuGridPMA Meeting
Lisbon, 6-8 October 2008

Info

- http://security.fi.infn.it/CA
- Since '99: grid (all Italy) & general purpose (INFN)
- Classical CA
  - user, server, service, robot
- 3150 valid certificates (30/9/08)
- 103 RAs
- Staff
  - 3 operators
  - 1 system manager (vacant)

The audit

- Three CA staff
- Two days
  - day 1: procedures and systems management
  - day2: disaster recovery
- Two external reviewers for the CP/CPS

Framework:
“Guidelines for auditing Grid Cas”
1.0-b4 (October 17, 2007)

Summary

Item #	description		
5	RFC 3647	open	disagree
15 & 16	CA key changeover	open	disagree?
32	CRLs version 2	open	next CP/CPS
37	Single network entity	closed?	
43	re-key vs renewal	closed	
50 (CA)	auditing CA staff	?	
50 (RA)	auditing RA staff	?	
51	List of RA personnel	closed?	
58	DIsaster recovery	open	January 2009
RA-4	Owner of the FQDN	open?	
RA-6	DN for the life	closed	some issues
RA-9	RA archives	closed?	kept by tha CA

Item 5

- “The CP/CPS document should be structured as defined in RFC 3647”
  - I don't think that the advantages of the new format justify the conversion effort
  - disagreement

Item 15 & 16

- “When the CA's cryptographic data needs to be changed, such a transition shall be managed […]”
  - We had already two cert changeover, but the procedure isn't well documented in the CP/CPS
  - Is the CP/CPS the right place to document this?

Item 32

- “The CRLs **must** be compliant with RFC3280, and is **recommended** to be version 2”
  - We'll change at the next CP/CPS revision
  - if compliance with RFC3280 is a must than version 2 is a must too

Item 37

- “Each host certificate must be linked to a single network entity”
  - The CP/CPS specifies that the DN must be a FQDN registered in the DNS
    - is this enough?

Item 43

- “Certificates […] managed in a software token should only be re-keyed […]”
  - Caught a bug in the control procedure
    - found 8 **renewed** certificates (not for grid), now revoked.

Item 50 (CA Staff)

- “Every CA must perform operational audits of the CA […] staff at least once per year”
  - Not clear what it means
  - Three personnel roles
    - manager;
    - operator;
    - system manager (vacant).

Item 50 (RA Staff)

- “Every CA must perform operational audits of the RA […] staff at least once per year”
  - Absolutely impossible (more that 200 people)
  - RA sign a document where he swears to behave well…

Item 51

- “A list of […] RA personnel should be maintained and verified […]”
  - An RA is nominated by his “manager”, typically in charge for 24 months
    - a renewal every change of manager?
    - minimum two RAs, each one guarantees for the other (since November '08);
    - a renewal every 5 years?

Item 58

- “The CA must have an adequate compromise and disaster recovery procedure [...]”
    - Work in progress

Item RA-4

- “The RA should ensure that the requester is appropriately authorized by the owner of the FQDN [...]”
  - Specified in the CP/CPS and in the document signed by the RA, but we don't know the details of the vetting procedures
    - insert details in the above documents?

Item RA-6

- “Over the entire lifetime it [subject DN] must not be linked to any other entity”
  - A problem with the older users, before we began keeping detailed info (“fiscal code” or date & location of birth)
    - we signal a possible conflict to the RA during the *de visu* authentication and let him decide

Item RA-9

- “The RA must record and archive all requests and confirmations”
  - RAs swear to do so, but we cannot verify (see Item 50)
    - CA has a copy, of course
  - RAs don't keep user data, apart name and email (privacy concerns)
    - CA keeps
      - “fiscal code” / date and place of birth
      - details of the ID document

Disaster Recovery

Status

- Work in progress
- First version for January '09
- NIST 800-53: Contingency Planning
  - low with a little of mod
- NIST 800-34

NIST 800-53: Contingency Planning

- CP-1: CONTINGENCY PLANNING POLICY AND PROCEDURES
- CP-2: CONTINGENCY PLAN
- CP-4: CONTINGENCY PLAN TESTING AND EXERCISES
- CP-5: CONTINGENCY PLAN UPDATE
- CP-6: ALTERNATE STORAGE SITE
- CP-7: ALTERNATE PROCESSING SITE
- CP-8: TELECOMMUNICATIONS SERVICES
- CP-9: INFORMATION SYSTEM BACKUP
- CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Backups

- Backup of keys in another building and off-site
- Sealed copies of passphrases and safe combinations off-site (a different one)
- Daily backups of on-line system (one off-site)
  - encrypted and signed (pgp...)
- Weekly backup of off-line system
  - kept in another building and off-site (TBD)
- Operations can be restored even if all CA staff disappear and the site is destroyed
  - documentation missing!
  - URL and email location-independent

Other Points

CP/CPS

- Many (minor) corrections to CP/CPS
    - next CP/CPS version
- The PMA must be revised

HW & SW

- Online system
  - software upgrade procedure
    - OS switch from FreeBSD to Debian
    - virtualization?
  - integrity check & log monitoring
    - OSSEC
  - resource planning
- Offline system
  - software upgrade procedure