Self-audit for Russian Data-Intensive Grid CA

Eygene Ryabinkin
EUGridPMA meeting in Riga
April 20th 2010

CA overview

- RDIG CA was established in 2005.
- Serving the Russian Data-Intensive Grid society, including people from JINR collaboration.
- Used to backup ex-USSR countries while they were establishing their own CA (Ukraine, Kazakhstan).
- Took over the Russian DataGrid CA that was operated by Lev Shamardin from SINP MSU.

CA operations: users and RAs

- We have RAs in all organizations that are eligible to get the certificates from our CA; large organizations have two or three Ras.
- In order to add new RA, organization should write official letter to the RDIG CA manager and the chief of the RDIG; this letter duplicates some data from the user's request in order to build the bridge between organization and its RA's certificate.

Certificate workflow

- Web interface is used to give the user keypair creation script and the paper form.
- User generates key material, sends the request to the public interface and fills the paper form where he signs the statement that he read and understand the CP/CPS.
- He visits his local RA with the paper form and some kind of the photo ID: passport, local institutional ID. RA verifies request, user's eligibility to get the certificate and signs the approval/rejection message with S/MIME.

Certificate workflow, part 2

- Signed request comes to the public CA interface where it gets verified and if verification succeeds, it is injected to the «signed» queue.
- CA operator transfers all signed requests to the offline signing host. Here requests are once again checked, RA's signature is verified and request is processed.
- All processed requests (along with the certificates) are transferred back to the public interface and mailed to the users.

Signing host

- Runs custom software that builds upon OpenSSL.
- Pure offline host; has all its data encrypted with the Blowfish; boot partition integrity is verified on the each boot.
- Technically, signing host is the external USB drive that can be plugged to virtually every PC that has USB and CD/RW (for backups).
- CA's private key and the disk itself are encrypted with the separate keys that have no less than 90 bits of entropy (Diceware).

Technical particulars of the signing host

- Running CD backups for every single signing session; backing up all data, but the CA private key.
- Restore is a simple process; moreover, building offline host from scratch is a simple process too: I had done it twice in the real-world conditions when USB disks were failed.
- Disk encryption: Blowfish with 256 bit key provided by the FreeBSD's geli(8).

Additional operations on the offline host

- CRLs are refreshed each time when certificates are signed; since we have 3 days to sign a single request by our CP/CPS and there was no single week when we had no requests, CRLs are refreshed no more than each 10 days; typical value is two days.
- Time is synchronized via the external GPS reciever and manually verified via host that is running NTP time sync. Time delta used for data transfer provides some space to make the certificates/CRLs to be valid (in respect to their issuance time).

Some facts

- Up to today, we had signed 2276 certificates, roughly two thirds of them were host ones and the rest consists of personal certificates.
- Currently (20.04.2010), we have 670 active certificates:
  - 241 user certificates;
  - 426 host certificates;
  - 3 service certificates.
- We had moved to the CN=<FQDN> at the previous year, but we do still support old CN=host/<FQDN> names.

RAs and auditing

- Each RA signs the paper form for each request he processes. He logs processing result, reason for such a result and signs (with pen) each form.
- On the regular basis, RA deliver all paper forms back to the CA operator. These forms are thoroughly checked for the compliance with the RA workflow and are selectively validated against the requests stored at the CA offline host.

Exchange between CA interfaces

- External USB stick and SSH secure copy are used to bounce the data between public online CA interface and the signing host.
- Each piece of data is signed with the PGP key and the signature is validated on both ends.
- CA offline host imports all data for all requests back to the online hosts after each session, so if the data on the public interface will be somehow tampered, it will be restored during the next signing session.

Treatment of personal and backup data

- Currently we keep all the data (paper forms, backups, official letters, signing logs) from the beginning of the CA operations; no data was thrown away.
- Personal data is kept only on the offline signing host on the encrypted partition; paper documents are kept in safes to prohibit the general access to this data.
- We keep generally-accessible list of currently active certificates; e-mails in them are obfuscated to make spammer's life harder.

That's all

Thanks for you time!

Questions, comments? You're welcome!