RDIG CA self-audit: 2018

Eygene Ryabinkin

National Research Centre “Kurchatov Institute”

EUGridPMA meeting, Toloise, September 26th 2018

Overview

- Classic offline CA (CEDAR as per IGTF LoA)
- Operates since 2005, survived one root prolongation in 2015.
- Serves Russian Data-Intensive Grid community (basically, HEP and mega-science)
- Operated by National Research Centre “Kurchatov Institute”
- Long-term commitment is here: we do at least Tier-1 for ALICE, ATLAS and LHCb. And KI now has 4 Tier-2 sites. Non-LHC activities: XFEL, Belle II via its russian users.

НИЦ «Курчатовский институт»

Identity vetting

- Face-to-face meeting of end users and RA either in-person or remotely with further short in-person talk in “tricky” cases.
- Strict fact-to-face in-person meeting with new RAs; supplemented by official letter to RDIG CA from RA organization.
- IDs in use: national passport, institutional photo-ID.
- RAs are local to the organization; their obligations are to check ID, relation of person (or administrator and host/service) to the RDIG CA and to collect paper forms for electronic request validation.

НИЦ «Курчатовский институт»

Identifiers and paperwork

- Two-level per-organization naming: /OU=type/OU=org-domain/DN=identifier
- Persons are identified by first/last name, may be supplemented with the middle one and trailing distinguisher (when needed)
- Hosts/services are identified by domain (and service) name.
- RA does validation of domain name ownership and relation to the organization and “RDIG-ness”.
- Signed paper forms are collected by RAs, originals are then sent to the CA for the long-term storage (at least 3 years).

НИЦ «Курчатовский институт»

Request validation and communication channels

- Paper forms oblige user to enter first/last 10 digits of the public key modulus.
- RA checks if this part of the modulus and other data on the paper is equal to those, received electronically.
- RA signs all requests with S/MIME using his own certificate.
- CA checks all signed requests and refuses to process invalid ones any further.
- Offline machine re-checks the whole request chain and signatures at the time of request processing.

НИЦ «Курчатовский институт»

Systems security and access controls

- Offline machine is booted from the encrypted USB disk; AES-XTS with 256-bit key is used; disk passphrase is more than 40 characters long.
- Online machine (Web interface, initial request processing) is secured with the usual measures – firewall, proper OS patching, service minimization, code audit – and lives inside the guarded perimeter of Kurchatov Institute in a physically-secured hosting room (locks, video surveillance, building access controls).
- CA root is 2048 bit long, protecting passphrase is longer than 30 characters.
- Passwords are known only to a single person; backups are stored in 2 safes in the management's rooms.

НИЦ «Курчатовский институт»

Audits

- CA operators are watching for EUGridPMA/IGTF practices and tries to keep up with them.
- CA operators perform routine audits of RA actions, taking corrective measures as needed.
- CA operators talk to the end-users (when possible) and verify that local RA operate according to the requirements.
- CA operators collect paper forms from RA and processes them doing selective audit of records and RA practices.
- CA does self-audits, but is often late for their presentation to EUGridPMA.
- All CA practice/operational changes are reflected in CP/CPS with changes announced to the EUGridPMA mailing list and are taken through the peer-review process.

НИЦ «Курчатовский институт»

The rest

- Compromise/disaster recovery: is here, can talk about them, but not write that.
- Privacy/confidentiality: according to the local laws; in short – we're doing our best to collect only what's needed and avoid disclosing it unless really needed.
- No private key generation/storage (only CA/RA "own" ones) at the CA/RA sides.
- Revocation: if suspected (with end-entity contact) or known; less than 24 hours.
- CRLs: issued on each signing session, but with no more than 25 days between them; next update is set to "+31 days".
- Thinking on the new root with 4096-bit RSA key: ETA is around 2 years. May be 8192-bit?

НИЦ «Курчатовский институт»

Thanks for your attention!

Questions?

Suggestions?

Other stuff?

Welcome!

НИЦ «Курчатовский институт»