# RDIG CA self-audit report

Eygene Ryabinkin, rea@grid.kiae.ru
20th EUGridPMA meeting, Zagreb,
September 21st 2010

# Overview

- Self-audit was done in accordance with the GFD.169 guidelines.
- Official reviewers: Jens Jensen, Christos Kanellopoulos.
- Current audit document version is 1.3, last modified at August 5th, 2010.
- Summary: 61 grade A, 2 grade D and 3 grade X marks.
- I'll go over the whole checklist and will highlight all «hard» questions.

# GFD.169 checklist items: 1/17

- Every CA must have a CP/CPS.
  - http://ca.grid.kiae.ru/RDIG/policy/
- Single CA per country, large region, etc.
  - Yes, we are the country-wide CA.
- Every CA must assign its CP/CPS an O.I.D.
  - Yes, OID come from IANA-registered subspace of 1.3.6.1.4.1.22139 – .1
- Changes in CP/CPS → changes in OID and announcement of major changes to PMAs
  - Yes, change procedures are in the section 8 of our CP/CPS.

# GFD.169 checklist items: 2/17

- All CP/CPS must be available on the Web.
  - Yes, http://ca.grid.kiae.ru/RDIG/policy/index-eng.html
- CP/CPS structure must conform to RFC 3647.
  - No, we're currently using RFC 2527
- Secure environment with controlled access to CA system.
  - Yes, CA is situated within the Kurchatov Institute and its territory is guarded with regular army; we have dedicated room with controlled access.

# GFD.169 checklist items: 3/17

- Offline CA system.
  - Yes, CA is completely offline.
- Minimal CA key length – 2048 bits.
  - Yes, exactly 2Kbits
- Long-term use for CA key.
  - Current expiration date – August 2015
- Software-based CA should have password with more than 15 characters and it should be known only to the designated personnel.
  - Yes, we're using Diceware-like approach with 67.5 bits of entropy for our password

# GFD.169 checklist items: 4/17

- Copies of encrypted private key must be secured.
  - Two distinct copies are kept in two safes on the territory of Kurchatov Institute
- Private key passprase must be kept in a secure location
  - Another safe within the same territory
- The on-line CA architecture...
  - Not applicable: we're offline CA
- Managed transision of CA crypto data
  - We're weak here: no current plans of any sort

# GFD.169 checklist items: 5/17

- The overlap of an old and a new key...
  - Not applicable: we don't have old and new keys.
- Distribution of CA certificate.
  - Yes, published in EUGridPMA repository, available on the Web
- CA's certificate lifetime < 20 years
  - Yes, 10 years
- CA's cert lifetime > 2x EE-cert lifetime
  - Yes, 10 years vs 2x 1.08 years
- CA cert profile must comply to GFD.125
  - Yes, it is GFD.125-compliant

# GFD.169 checklist items: 6/17

- Persons that can request revocation.
  - Usually, all goes through the respective RA; but we deal with other cases on the per-request basis
- Revocation request must be processed in one working day.
  - Yes, we're trying to do our best and had never delayed processing up to date
- Subscribers must request the revocation within one working day
  - Our clients are bound to it by our CP/CPS and the document they are signing for each request

# GFD.169 checklist items: 7/17

- Authentication of revocation requests
  - S/MIME (primary method), PGP for applicable cases
- Generation and publishing of CRLs
  - Yes:
    - http://ice.grid.kiae.ru/ca/RDIG/cacrl.pem
    - http://ca.grid.kiae.ru/RDIG/cacrl.pem
- CRL lifetime <= 30 days
  - 30 days sharp
- CA must issue new CRL 7 days before the old one will expire.
  - New CRL issued at each signing session

# GFD.169 checklist items: 8/17

- Immediate CRL issuance after revocation
  - Again, each signing session → new CRL
- CRL must be published as soon as issued
  - Yes, it is published within 5 minutes at http://ice.grid.kiae.ru/ca/RDIG/cacrl.pem
- CRLs must be complicant with RFC 5280.
  - Yes, they are
- User/host key length >= 1024 bits.
  - Exactly 1024 bits
- User/host cert lifetime <= 13 months
  - EE certificates have lifetime of year and a month

# GFD.169 checklist items: 9/17

- No user certificates may be shared.
  - Users are obliged through the CP/CPS and the document they are signing for each request
- EE cert cryptographic data origin is the request applicant.
  - Yes, RDIG CA never generates keying material to its users
- Assurance that subscribers are properly protecting their private data.
  - It is clearly stated in the CP/CPS, paper form for certificate request and explanation is displayed during the generation of the new request

# GFD.169 checklist items: 10/17

- EE certificates must be GFD.125-compiant.
  - Yes, they are
- CommonName should carry actual end-entity name.
  - DN contains person's first and last name, as per CP/CPS, section 3.1.1
- Software-based stuff shouldn't be renewed.
  - We're checking for the reusal of private keys and prohibiting such requests
- Hardware-based stuff...
  - Not applicable: we don't use it

# GFD.169 checklist items: 11/17

- Auditable re-keys/renewals.
  - *Each* request is validated through RA
- Archival of all CA logs.
  - We're making backups of all CA stuff at the end of each signing session using CD-R media; we also have paper-based session logs as the backup
- Logs must be available for the auditors.
  - Yes, but in-person presence at the RDIG CA facilities is required
- Logs are to be kept for >= 3 years
  - We're not purging any archives

# GFD.169 checklist items: 12/17

- Acceptance of external audit by other CAs.
  - Yes, CP/CPS, section 4.5. In fact, we're doing it just now ;)
- Operational audits of CA/RA staff.
  - Internal audits are performed at least once per year, on ocassion, they are performed even more frequently
- A list of CA/RA personnel should be maintained and verified at least once a year.
  - http://ca.grid.kiae.ru/RDIG/requests/ra-list.html, RA data is checked at each internal audit

# GFD.169 checklist items: 13/17

- Repository availability – best effort with the target of 24x7.
  - Yes, http://ca.grid.kiae.ru/RDIG/ is maintained with these goals in mind
- Publishing of AA root of trust.
  - Yes, our root is published by EUGridPMA/IGTF
- Publishing of CA metadata for subscribers, RPs, etc.
  - Yes
- Unlimited redistribution of the metadata.
  - Granted by lack of distribution restrictions

# GFD.169 checklist items: 14/17

- Root-of-trust integrity validation.
  - SHA1 fingerprint is published by EUGridPMA/IGTF
- Availability of trust anchor in the trust anchor repository.
  - Available in the EUGridPMA/IGFT repositories
- Privacy and data release policy.
  - We have one, CP/CPS, section 4.6
- Adequate compromise and disaster recovery procedure.
  - It is outlined in section 4.8 of CP/CPS

# GFD.169 checklist items: 15/17

- Existence of a proper RA roles.
  - Each domain has its RA(s), they check and authenticate requests and their holders, including the eligiblity to have RDIG CA certificate
- Face-to-face meeting of requestor with RA.
  - Yes, we're doing exactly this
- Validation of identity and eligibility for non-personal certificate requests.
  - Outlined in the RA instructions and section 2.1.2 of CP/CPS; basically, the same process as for personal certificates

# GFD.169 checklist items: 16/17

- Authorization from FQDN holder for host and service requests.
  - RA does it using the local DNS authority
- Verification of an association of CSR.
  - RA does it by comparing the personal data and public key modulus at the paper form and incoming request to be processed
- Evidence on identity retainment.
  - RA checks national or institutional photo-ID
- Any single DN must be linked to one entity.
  - Yes, expanded (and long) explanations are in the self-audit document

# GFD.169 checklist items: 17/17

- Secure communications between CA and RA
  - RA use S/MIME messages to approve/reject requests and to generate revocation requests
- How CA/RA are informed of changes that may affect the status of the certificate.
  - Section 4.4.3 of CP/CPS, basically it is the revocation policy
- Archives of RA stuff.
  - Done by the RA utility software
- Auditable archive of RA records on the CA.
  - Yes: signing host have all of them

# Wow, it is finished!

Well, that's all!

Any questions, comments, additions?

Thanks for your time!