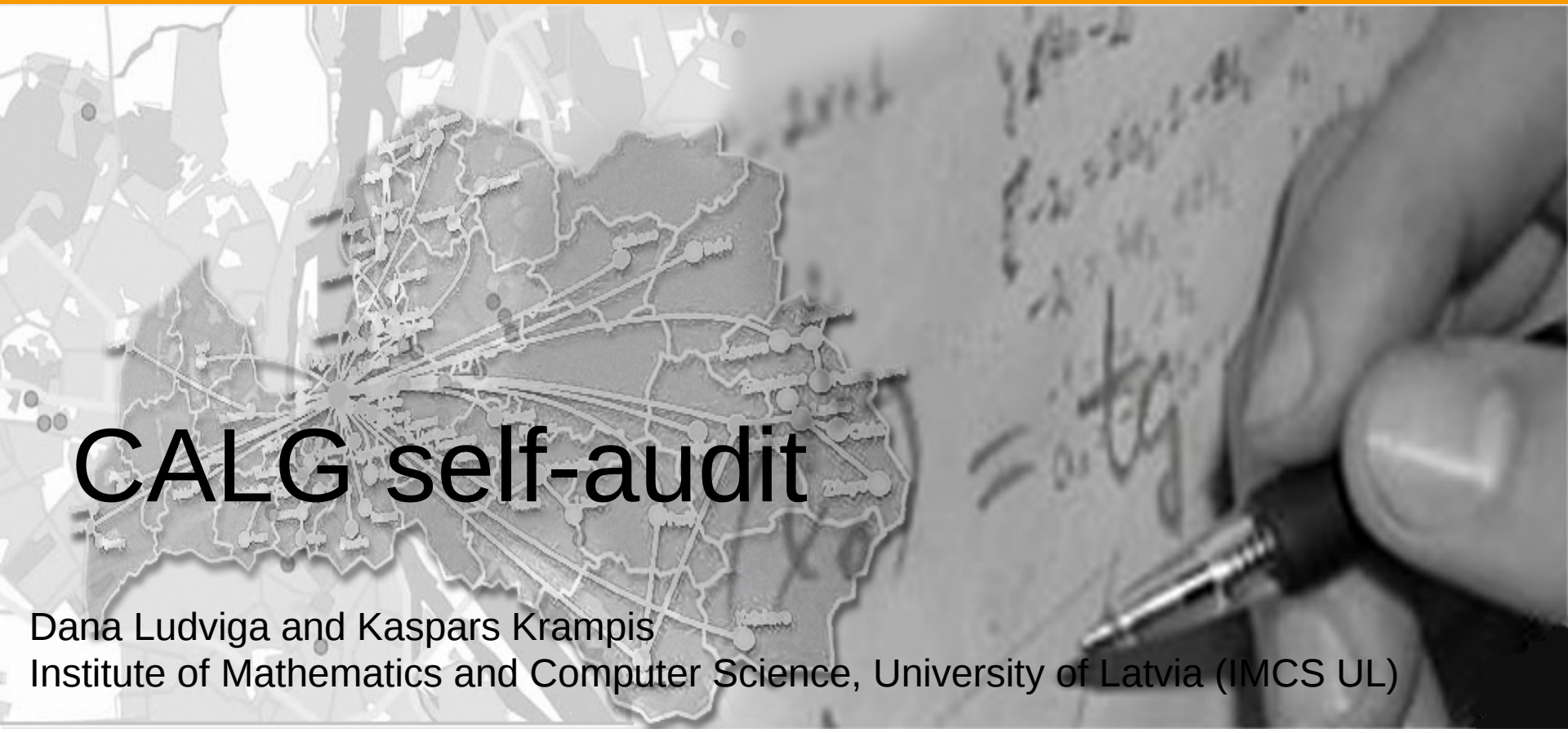


CALG self-audit

Dana Ludviga and Kaspars Krampis
Institute of Mathematics and Computer Science, University of Latvia (IMCS UL)

28th EuGridPMA, Kyiv, Ukraine
May 13, 2013

Overview

- CALG
- Self-audit:
  - Recommendation (minor changes)
  - Recommendation (major changes)
  - Could not evaluate
- Conclusions

CALG: Certification Authority for Latvian Grid

28th EuGridPMA, Kyiv, Ukraine
May 13, 2013

CALG

- CALG provides PKI services for grid initiatives in Latvia
- EuGridPMA accredited in 2009
- Managed and funded by IMCS UL
- Operated by:
  - Dana Ludviga (leaving soon for a year or two)
  - Kaspars Krampis
  - Mārtiņš Lībiņš
  - Leo Trukšāns

CALG self-audit

28th EuGridPMA, Kyiv, Ukraine
May 13, 2013

Self-audit

- Document used:
  - GFD-I. 169 (April 19, 2010)

- Overview:
  - 46 A: Good
  - 8 B: Recomendation (minor change)
  - 2 C: Recommendation (major change)
  - 10 D: Advice (must change)
  - 2 X: Could not evaluate (N/A)

B: Recommendation (minor change)

B (minor change)

- 3.1.1(6) The CP/CPS documents should be structured as defined in RFC 3647
  - CALG CP/CPS currently is structured as defined in RFC 2527

- 3.1.1(11) The CA key must be configured for long term use
  - The CALG private key has a validity of 10 years (stated in section 6.3 not 6.3.2)

B (minor change)

- 3.1.1(12) If the private key of the CA is software-based, it must be protected with a pass phrase of at least 15 elements and it must be known only to designated personnel of the CA...
  - CALG CA private key is protected by 15+ element passphrase, passphrase is known only to designated CA personnel.
  - The multi-person control is not implemented, thus B.

- 3.1.1(19) Lifetime of the CA certificate must be no longer than 20 years.
  - Mentioned in section 6.3. (not 4.7.)
  - Inspection: CA certificate has a lifetime of 10 years, valid till 2018.

B (minor change)

- 3.1.1(23) The CA must react as soon as possible, but within one working day, to any revocation request received.
  - Section 4.4.4 (not 4.4.3)

- 3.1.1(28) Every CA must issue a new CRL at least 7 days before the time stated in the nextUpdate field for off-line CAs, at least 3 days before the time stated in the nextUpdate field for automatically issued CRLs by on-line CAs.
  - Inspection: CA has missed 7 day deadline on several occasions. Thus **B**.

B (minor change)

- 3.1.1(29) Every CA must issue a new CRL immediately after a revocation.
  - Inspection: Multiple revocation requests are processed in single CA room and equipment access session and single CRL is issued for all revoked certificates at once.

- 3.1.1(36) Every CA should make a reasonable effort to make sure that subscribers realize the importance of properly protecting their private data...
  - Section 2.1.3 not 6.2.7

C: Recommendation (major change)

C (major change)

- 3.1.1(9) The secure environment must be documented and approved by the PMA, and that document or an approved audit thereof must be available to the PMA. Can be covered by the auditing item (7).
  - The secure environment is documented by the CP/CPS (section 5.1.). Select EUGridPMA members have visited and seen it (David G., Hardi T., Christos K.).

- 3.1.1(24) Subscribers must request revocation of its certificate as soon as possible, but within one working day after detection of he/she lost or compromised the private key pertaining to the certificate or the data in the certificate are no longer valid.
  - Nothing mentioned in CP/CPS about ASAP/1 working day.

D: Advice (must change)

D (must change)

- 3.1.1(20) Lifetime of the CA certificate must be no less than two times of the maximum life time of an end entity certificate.

and

3.1.1(33) Lifetime of user certificates and host certificates must be no longer than 13 months.

  - CP/CPS doesn't include the lifetime of end entity certificates.
  - Inspection: CA certificate has a lifetime of 10 years. EE certificates have lifetime of 1 year.
  - Action: Add the maximum validity period (395 days) for a certificate in section 4.7.

D (must change)

- 3.1.1(31) The CRLs must be compliant with RFC5280.
  - CRLs are generated in x.509 v1, should upgrade to x.509 v2 and change CP/CPS section 7.2.1.

- 3.1.1(37) The end-entity certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125....
  - Certificate must include the OID or Authentication Profile under which the Certification Authority has been accredited. For Classic AP, OID is 1.2.840.113612.5.2.2.1.

D (must change)

- 3.1.1(40) Certificates associated with a private key residing solely on hardware token may be renewed for a validity period of up to 5 years (for equivalent RSA key lengths of 2048 bits) or 3 years (for equivalent RSA key lengths of 1024 bits).
  - CP/CPS doesn't include this requirement

- 3.1.1(41) Certificates must not be renewed or re-keyed consecutively for more than 5 years without a form of auditable identity and eligibility verification, and this procedure must be described in the CP/CPS.
  - CP/CPS doesn't include this requirement. At the moment only the proof of relation with the organizations mentioned in the certificate subject name is checked upon a rekey request.

D (must change)

- 3.2.1(2) and 3.2.1(3) regarding RA identity validation procedure
  - Section 2.1.2. states, that RA must collect a copy of some kind of identification document (passport or drivers license). According to the changes in the governing law of Latvia, we have no right to make a copy of an identification document. Instead we have developed a special form where we record data - document type (passport or driving license), number, issuing date, validity date and issuing body.

- 3.2.1(6) and 3.2.4(9) regarding CA or RA documented evidence and its' archival
  - Section 4.6.1 states that RA should also record a copy of all personal data documents mentioned in section 2.1.2.

X: Could not evaluate (N/A)

X: Could not evaluate

- 3.1.1(2) Is there a single CA organisation per country, large region or international organization?
  - No, Latvia is also covered by the BalticGridCA
  - This was discussed and taken into account by the EuGridPMA when accrediting CALG

- 3.1.3(15) The on-line CA architecture should provide for a (preferably tamper-protected) log of issued certificates and signed revocation lists.
  - CALG is not an on-line CA

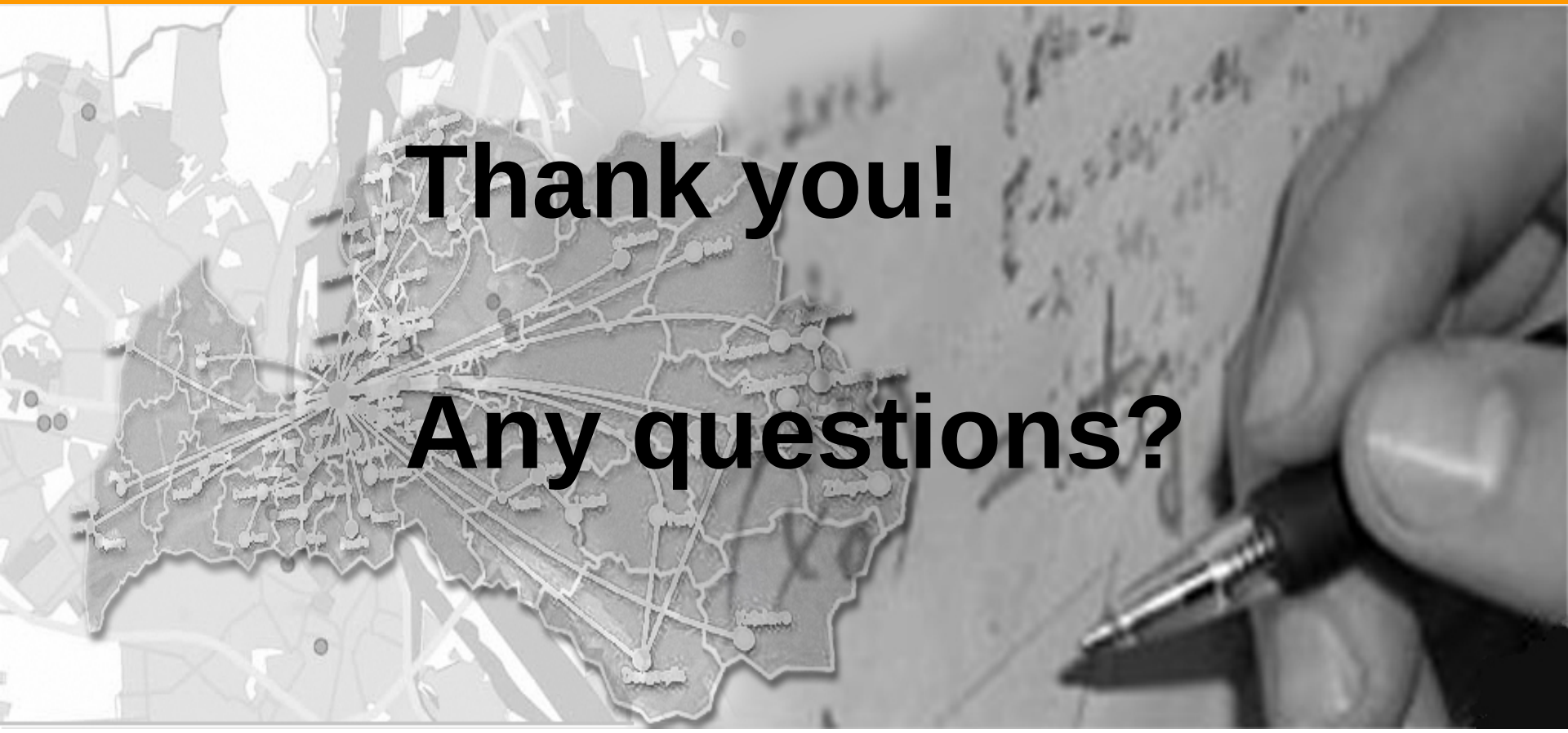
Conclusions

Conclusions

- CP/CPS needs to be updated
- CRLs version upgrade to x.509 v2
  - Starting from next issued CRL
- Include the OID 1.2.840.113612.5.2.2.1 in end-entity certificates
  - Starting from next issued EE certificate

- Additional changes:
  - Switched from Knoppix to Ubuntu LiveCD

CALG - CA Latvian Grid



28th EuGridPMA, Kyiv, Ukraine
May 13, 2013