# SlovakGrid Certification Authority update & audit results

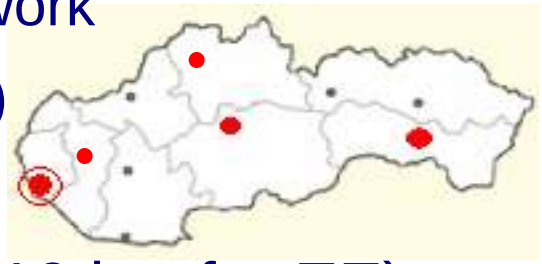
Miroslav Dobrucký
IISAS
Department of Parallel and Distributed Computing
**Institute of Informatics**
Slovak Academy of Sciences
http://www.ui.sav.sk

# Overview

- SlovakGrid CA
- Latest operational changes and Statistics
- CP&CPS major update (2009-…)
- Self-audit results
- Plans

# SlovakGrid Certification Authority

- Managed by IISAS, Bratislava, Slovakia, since Dec'02
  - issues EE certificates for subjects related to organizations in Slovakia and involved in research or deployment of Grids
- **Classic**, based on openssl + custom scripts (CA.pl)
- Certificate issuing machine:
  - located in a room with restricted access
  - in locked case, never connected to any network
  - managed by CA operator (me or my deputy)



- 5 registration authorities established ( < 110 km for EE)

# Off-line CA-system

# SlovakGrid CA root certificate

- Private key is 2048 bits long
- Encrypted by passphrase >15 characters
- CA certificate lifetime 20 years (2002-2022)
- Backup copy of the private key and sealed envelope with the passphrase are locked separately in a safe places
- Will be rekeyed before November 2021

# Information publishing

- SlovakGrid CA online repository contains:
  - SlovakGrid CA root certificate
  - Latest CRL
  - Copy of CPS/CP document (actual and all previous)
  - Other relevant information
    - list of RAs
    - list of used O names
    - CA postal address
- URL: http://ups.savba.sk/ca/

# Overview

- SlovakGrid CA
- **Latest operational changes and Statistics**
- CP&CPS major update (2009-…)
- Self-audit results
- Plans

# Latest operational changes

- 4-th RA created in Žilina (May'09, north-west SK)

Mar'10:

- Personal change in 3-rd RA in Banská Bystrica (mid SK)
- 5-th RA created in Trnava (west SK)

Sep'11:

- CA root certificate lifetime 20 years (5->10->20)

Oct'12:

- HW upgrade (SL6), old disk with CA-key re-used
- SHA2 operational since October, we are waiting for "GO!"

Jan'13:

- CRL published format changed to DER
  - Many of EGI-trustanchor CAs still publish PEM (44 of 103)

# Certificates: statistics

For whole period 17 Dec 2002 – 14 Jan 2013:

**988** end entity certificates have been issued

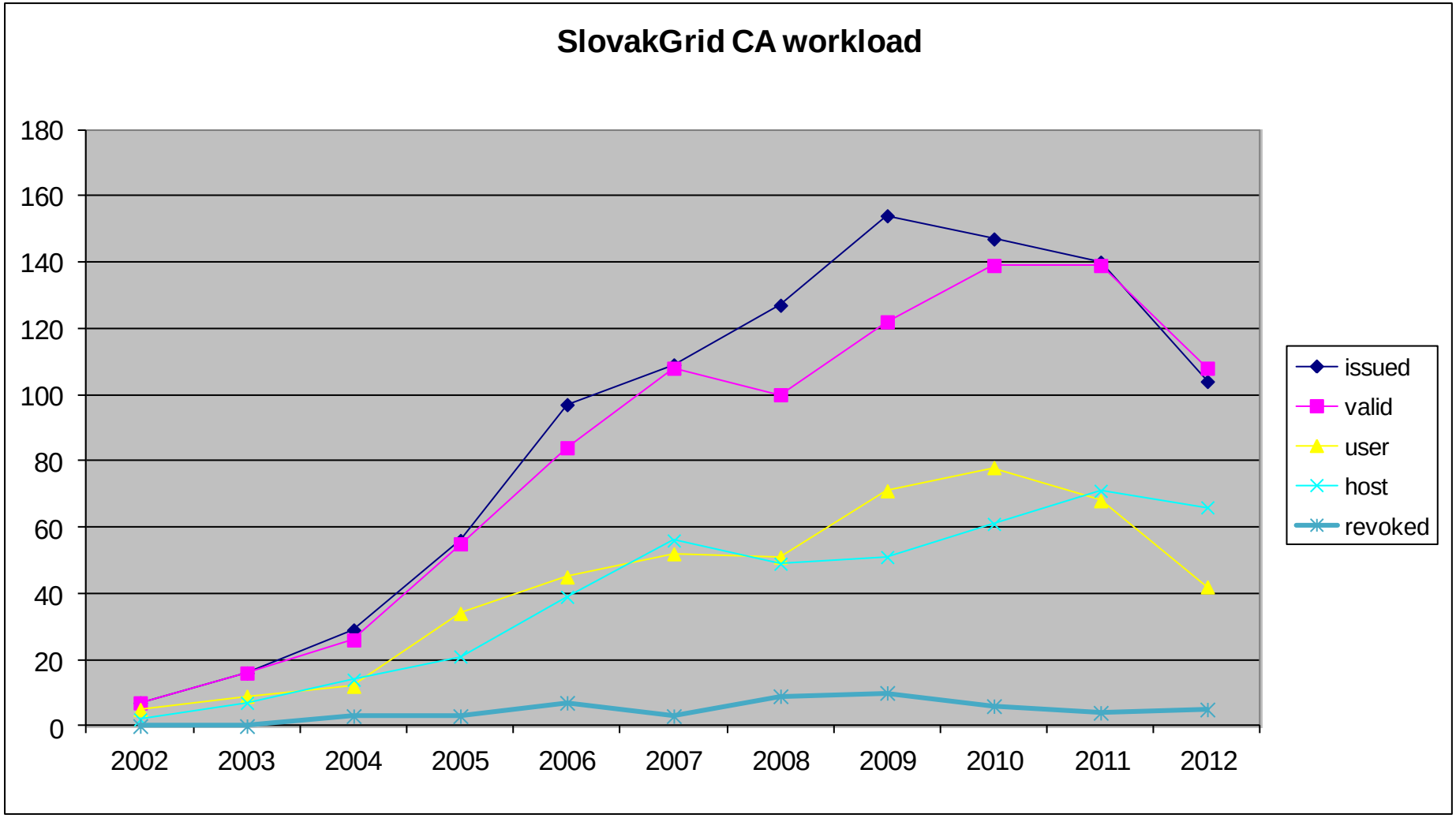
50 have been revoked (user 25, server 25)

Unique subject DNs: **337**

Status on 14th January 2013:

**110** are valid (user 42, server 68)

# Certificates: workload



# Overview

- SlovakGrid CA
- Latest operational changes and Statistics
- **CP&CPS update (2009-…)**
- Self-audit results
- Plans

# ‘New’ CP/CPS – to be published

Version 2.1 (major update, presented in 12th EUGridPMA, 2008)

- OID: 1.3.6.1.4.1.13496.1.2.1.2.1

- Reviewed by Emir (5 May 2009), but still not published ☹
- based on minimal requirements IGTF-AP-classic-v4.1
- based on self-audit results (Dec’07)

**Major changes** (compared with v1.2, June 16, 2003):

- Private key passphrase required length ≥ 12 (was ≥8, Feb’06)
- CA root certificate lifetime 10 years (was 5, Jan’07)
- EE cert’s lifetime 13 months (was 12, used 13m since Jan’07)
- Added “rekey without F2F authentication at most 5 years”
  - followed in practice, no user complained for “obsoleted CP&CPS”

# ‘New’ CP/CPS …major changes

- Authentication of a server/service certificate request is possible without F2F
- Sending a request for user cert by e-mail is recommended (must ->should, text added: for pre-checking purpose)
  - Text added: “and must be delivered by secure way (e.g. personally on removable media) to indicated RA”
- Added CA obligation: revoking within 1 working day = best effort basis
- Added user obligation: notify CA within 1 working day if key compromised
- CA private key is kept separately from the passphrase (this reflects the reality since 2002)
- Added: “user may ask for additional certificate with extended DN”
- Added user obligation: “Issued certificates must not be shared”
- Added RA obligation: “Maintain the list of records with subscriber signatures affirming acceptation of the policies and procedures published in this document;“
- secure RA/CA communication is specified

# ‘New’ CP/CPS …minor changes

Minor changes:

- Change in the contact person (Jan Astalos -> me)
- Change in e-mail adress (@savba.sk -> @sav.sk, alias -> mailinglist)
- 2.8.3. b) “The requester of the server or service certificate;” (enhanced)
- 3.2 “Expiration warnings will be issued to subscribers when rekey time arrives, usually 1 month ahead. “ (enhanced)
- 4.4.5 Removed suspension possibility (never used in reality)
- 4.4.8 “reissued and at least“ -> “reissued at least“ (typo)
- 4.5.3 “Logs will be kept for a minimum of 3 years” added: “, where the identity validation records must be kept at least as long as there are valid certificates based on such a validation. “ (i.e. >5years).
- 6.1.3 “floppy disk.” -> “floppy disk or using other removable media.”

# ‘New’ CP/CPS …minor changes

Further minor changes:

- 6.4. Added: “Changes of CA private key passphrase are done according to the security needs, i.e. when CA personnel is changed/left/retired.”
- 7.1.4-5 “*countryName*” -> “SK” (not an option, text simplified)
- 7.1.2 “*policyIdentifier*” added; “CA”->”CA:true”, “Not a CA”->”CA:false”
- And other minor changes reflecting the self-audit results (approval policy, all CPS present on the web, yearly operational audits, …)

Other ‘news’:

- User-relevant part of CP&CPS was translated to Slovak language (v2.1)
- MD5/SHA1 digest of CP&CPS document was be published on the web
- Registered in TACAR (at 12th PMA meeting in Amsterdam 2008)

# Overview

- SlovakGrid CA
- Latest operational changes and Statistics
- CP&CPS update (2009-…)
- **Self-audit results**
- Plans

# Self-audit results (Dec'07)

7 "must change" items (D)

6 major change recommendations (C)

18 minor change recommendations (B)

86 good items (A)

18 N/A items (X) (no hw module used, no certificate profile, not on-line CA, no CA rekey in the past, no user manual, no operational manual, etc.)

---- Auditor: myself

135 Done according to the AuditGuidelines-1.0b4.doc , 17 Oct 2007

# Self-audit results (Jan'13)

2 "must change" items (D)

1 major change recommendation (C)

10 minor change recommendations (B)

89 good items (A)

14 N/A items (X) (no hw module used, not on-line CA, no CA rekey in the past, no user manual, no operational manual, etc.)

---- Auditor: myself

**117** Done according to the GFD.169 (AuditGuidelines-1.1, 28 Oct 2010)

Audited CP&CPS **v2.1 supposed as to be accepted.**

Note: All **sub-items** count = 117.

# Self-audit results (Jan'13)

1 "must change" items (D)
1 major change recommendation (C)
7 minor change recommendations (B)
56 good items (A)
2 N/A items (X) (no hw module used, not on-line CA)

---- Auditor: myself

**67** Done according to the GFD.169 (AuditGuidelines-1.1, 28 Oct 2010)

Audited CP&CPS **v2.1 supposed as to be accepted.**

Note: Numbered items count = 67.

# MUST change (D: 1 item)

- Auth.Profile v4.3: *policyIdentifier* in the EE-cert ...MUST include at least the OID for the Classic profile: 1.2.840.113612.5.2.2.1
  - Our certs have only our **CA-**CP&CPS OID in this extension !
  - Solution: -> will be added in next CP&CPS update
    - Will be added to new EEs

Note: APv4.3 : EE may include **CA-**CP&CPS OID

- GFD.169: check-point 37i: **must**

# Major change (C: 1 item: **5 major-**sub-items)

- Remove CRL distribution point in CA-cert
- Remove CP&CPS URL in CA-cert (ns* extension)
- Remove all other *nsCertType* in CA-cert
- Remove Serial and DirName in CA-cert (but how?)
- Remove “Non Repudiation” in EE-cert *keyUsage*

- Solution: -> all 5 items will be removed in next CP&CPS update

# Major change (C: 1 item: **5 minor-**sub-items)

- Remove “Digital signature” and “Non Repudiation” in CA-cert *keyUsage*, remove *“objectSigning”* in EE-certs ->rm
- Remove Serial and DirName in EE certs (GFD.125 allow this in 3.3.9) and in CA-cert ->rm
- Change DN from starting “C=“ to “DC=” (34 CA-certs in EGI-trustanchors have DC, 68 have C)
  - -> in case of new CA-cert (if SHA2 needs it)
- Remove ns* in CA and EE-certs
  - *extendedKeyUsage* is preferred over *nsCertType*
  - verify if *nsCertType* is needed for MON node ->rm of OK
- CN=host/* recommended not to use by GFD.125 note 25 **OK**

# Minor change (B: 7 items)

- CA-room acess log is not performed (no guard installed)
- CA-cert lifetime prolonged from 10 to 20 years ->update CPS
- yearly operational audits not auditable (no logs and not done so often, Solution -> write minutes of audits
  - operational manual does not exist -> write manual
- (3x) RA should have documented evidence on retaining the same identity over time ( -> write-down birth dates)
  - user manual does not contain check-points 40-42 ->update UM
- an adequate compromise and disaster recovery procedure  missing -> write procedure
- CRL compliace with RFC5280 not fully checked ->hope is OK

# Overview

- SlovakGrid CA
- Latest operational changes and Statistics
- CP&CPS update (2009-…)
- Self-audit results
- **Plans**

# Minor update of CP/CPS document

Proposal: CP&SPC version 2.2 (minor update, 2013)

- based on minimal requirements IGTF-AP-classic-v4.3
- based on GFD.169 and GFD.125
- based on self-audit results (Jan'13)

- Write down users' birth dates in the identity vetting records
- Accept CSR with key length at least 2048 bits
- Follow GFD.125 recommendations:
  - Remove *nonRepudation* in server/service certificates
  - *extendedKeyUsage* instead of *nsCertType* (at least one must be present in EEcerts)
  - Remove all other not needed extensions
  - OID for the Classic profile will be added

# Further plans

- Change e-mail in CA and EE certs: @savba.sk -> @sav.sk
  - My alias -> mailinglist, which members are me + my deputies
- Write SlovakGrid CA Operations Manual (intended for RA)
- Update User manual (now only rekey procedure is on the web)
- Write an adequate compromise and disaster recovery procedure
- pk-protection-1.1-20100921.doc:
  - UI-node should have a legal status, documents (it holds users' keys although not in plain text)
  - UI-node should sit in secured room

# Thank you.

ca.ui {at} sav.sk

Miroslav.Dobrucky {at} savba.sk