MARGI CA Self Audit

Bozidar Proevski

MARGI

R. Macedonia

Overview

- MARGI CA
- Self Audit
  - Certification Authority
  - Registration Authority
- Conclusion

MARGI CA

Overview

- Established in April 2005
- Serves the Macedonian academic and research community
- Public web site: http://www.margi.marnet.net.mk
- Email address: margi-ca@margi.marnet.net.mk
- Approved by EUGridPMA in January 2008
- Single CA for Macedonia

Organization

- **CA & RA @ MARGI CA**
  - One CA: Boro Jakimovski (was Aleksandar Dimeski)
  - One RA: Bozidar Proevski
  - The change of contact person is in the proposed CP/CPS update

MARGI CA is hosted at the Faculty of Computer Science and Engineering

- Since MARNET has evolved into a governmental agency, MARGI CA must change the trust anchors
  - Not to include the domain *marnet.net.mk*
  - The new domain will be *margi.ukim.mk*

System Architecture

- CSP (http://devel.it.su.se/projects/CSP/)
- Dedicated offline machine (Raspberry Pi), which is kept in a locked place, only MARGI staff has access
- Offline commandline interface
  - EE certificate requests transferred on a separate medium
  - crude shell script automation
- Future alternatives
  - easy-rsa
  - TinyCA

CP/CPS

- Current version 1.0
- Issued November 10th 2007
- Took effect 14 January 2008
- OID 1.3.6.1.4.1.28430.10.1.1.0
- Conforms to RFC 3647

CP/CPS

- Proposed update will be version 1.1
- Issued September 10th 2014
- OID 1.3.6.1.4.1.28430.10.1.1.1
- Conforms to RFC 3647

Changes in CP/CPS

- Change of the O.I.D of the CP/CPS, to reflect the version change
- Subscribers must request revocation of its certificate within one working day, requirement was added in classic AP 4.1
- For Classic AP, add OID 1.2.840.113612.5.2.2.1 to the Policy

CA key

- 2048 bits RSA with SHA1
- Expires January 20 2028
- Copy on an offline medium (paper, CDROM, kept in a safe)
- Protected with a long passphrase, passphrase kept in a separate location

CA certificate

- Published in EUGridPMA
- GFD.125 Compliant

EE certificates and keys

- 2048 bits, RSA, SHA1
  - changes made to start issuing SHA512 signatures, but...
  - recommendations for a hash algorithm, 256 or 384?
- Lifetime is 13 months
- Each subscriber must generate his/her own key pair, but in practice gridadmins help with instructions if subscriber is not able to do it by himself.
- GFD.125 compliant

Issued certificates

- Total: 180 issued certificates
  - Host certs: 111 (30 unique hosts)
  - User certs: 69 (42 unique users)
- Valid: 19 certificates
  - Host certs: 15
  - User certs: 4
- Revoked: 1
  - Reason: private key was lost due to disk corruption

Certificate revocation lists

- http://www.margi.marnet.net.mk/CA/margi-v2.crl
- CRL is compliant with RFC 5280

Records archival

- All certificate requests are archived
- Currently there are no signed approvals due to the small community
  - all current users are faculty staff
  - all previous users were either faculty professors and staff or students known by the professors

Publication and repository responsibilities

- Repository is available at http://www.margi.marnet.net.mk/CA
- Root is published by EUGridPMA with SHA1 fingerprint
- Unlimited distribution of public data

Registration authority

- Currently one RA, due to small community

SELF AUDIT

Versions

- Guidelines for auditing Grid CAs version 1.0
  - GFD.169, April 19th 2010
- MARGI CA CP/CPS version 1.1
  - September 10th 2014

Summary

- Total number of items: 68
- Marks:
  - C: 1
  - B: 2
  - X: 1
  - A: 64

CERTIFICATION AUTHORITY

CA Key

- B – 3.16
  - Item description: The on-line CA architecture should provide for a (preferably tamper-protected) log of issued certificates and signed revocation lists.
  - Status: Logs of issued certificates are kept. Logs of CRLs are not kept. (Section 5.4.1)
  - Practice: Only the current CRL is published.
  - Solution: We will start collecting previous CRLs and publish them on the web repository.

End Entity Certificates and Keys

- X – 7.41
  - Item description: 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).
  - Comment: CA does not support keys residing on hardware tokens.

Records archival

- B – 8.43
  - Item description: Every CA must record and archive all requests for certificates, along with all issued certificates, all requests for revocation, all the issued CRLs and login/logout/reboot information of the issuing machine.
  - Comment: Related to previous B mark.

REGISTRATION AUTHORITY

RA to CA Communications

- C – 2.9
  - Item description: All communications between the CA and the RA regarding certificate issuance or changes in the status of a certificate must be by secure and auditable methods.
  - Status: Auditability is defined in section 5.5.1. Secure emailing should be added in section 9.6.1, section 9.6.2.
  - Practice: There are currently one CA and one RA. Communication between them is in person or unsigned email.

Conclusion

- There are several issues that mandate a change of the CP/CPS

Thank You!

Questions?