Karlsruhe Institute of Technology

EuGridPMA Meeting, Nicosia, 26.-28.01.2009
GridKa-CA Self Audit

Steinbuch Centre for Computing (SCC)
Ursula Epting

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft

Universität Karlsruhe (TH)
Forschungsuniversität • gegründet 1825

Outline

- The GridKa-CA
- How the review was done
- Classification
- Review results overview
- Review results details 'major' and 'must' changes
- Conclusion

The GridKa-CA

- Accredited since 2002 – first as 'FZK-Grid-CA', 2003 change to 'GridKa-CA' run by Forschungszentrum Karlsruhe GmbH (Germany)
- Issued 7770 certificates (valid about 3900, two third hosts)
- Now FZK is going to be merged with University of Karlsruhe to 'Karlsruhe Institute of Technology'.
- Former departement 'Institute for Scientific Computing (IWR)' has already changed to 'Steinbuch Centre of computing (SCC)' which combines the computing centres of FZK and University of Karlsruhe

  => Yet another name change, but this will not remain the only change in the CP/CPS...

How was the review done?

Review based on the following documents

- Guidelines for auditing Grid CAs version 1.0-b7 (1.0-b6 inside Document) from Yoshio
  https://forge.gridforum.org/sf/go/doc4858
- Relevant IGTF Authentication Profile(s)
  http://www.eugridpma.org/guidelines/IGTF-AP-classic-4-2.pdf
- Grid Certificate Profile document
  draft-ogf-caops-grid-certificate-profile-v27.doc
- RFC 5280
  http://tools.ietf.org/html/rfc5280
- RFC 3280
  http://www.ietf.org/rfc/rfc3280.txt
- Full report, documents and links will be given to reviewers (Jens Jense, Milan Sova)

Classification

- A = Good (green)
- B = Recommendation minor change (yellow)
- C = Recommendation major change (orange)
- D = Advice must change (red)

Review results overview

CA	Points	D (must change)
1. CP/CPS	6	(1),(2),(3), (5) (4) (6)
2. CA system	4	(9), (8) (7), (10)
3. CA Key	8	(11), (12), (13), (14), (15), (17) (18) (16)
4. CA certificate	6	(19), (20), (21), (22), (23) (24)
5. Certificate Revocation	4	(25) (26), (27), (28),
6. Certificate Revocation List	8	(29), (33), (36) (30), (31),(32) (34), (35)
7. End Entitiy Certificates and Keys	12	(37), (38), (41), (43), (45), (46) (42), (48) (44) (39), (40) (47)
8. Records archival	3	(51) (49) (50)
9. Audits	3	52), (54) (53)
10. Publication and Repository responsibilities	6	57), (56 (57) 58), (59) (60)
11. Privacy and confidentiality	1	61)
12. Compromise and desaster recovery	1	(62)
RA		
1. Entity Identification	5	(2), (1), (3) (4), (5)
2. Name Uniqueness	2	(5') (6)
3. RA to CA communication	2	(7), (8)
4. Records and Archival	2	(9), (10)
	73	73

Joke ;)

Real review results overview

CA	Points	A	B	C	D	unclear
1. CP/CPS	6	(1),(2),(3), (5)	(4)	(6)		
2. CA system	4	(9), (8)	(7), (10)			
3. CA Key	8	(11), (12), (13), (14), (15), (17)	(18)			(16)
4. CA certificate	6	(19), (20), (21), (22), (23)		(24)		
5. Certificate Revocation	4	(25)	(26), (27), (28),			
6. Certificate Revocation List	8	(29), (33), (36)	(30), (31),(32)	(34), (35)		
7. End Entitiy Certificates and Keys	12	(37), (38), (41), (43), (45), (46)	(42), (48)	(44)	(39), (40)	(47)
8. Records archival	3	(51)	(49)		(50)	
9. Audits	3	(52), (54)			(53)	
10. Publication and Repository responsibilities	6	(55), (56)	(57), (58), (59)		(60)	
11. Privacy and confidentiality	1	(61)				
12. Compromise and desaster recovery	1				(62)	
RA						
1. Entity Identification	5	(2),	(1), (3)			(4), (5)
2. Name Uniqueness	2	(5')	(6)			
3. RA to CA communication	2		(7), (8)			
4. Records and Archival	2	(9), (10)				
	73	37	21	5	6	4

C - major changes in CP/CPS

(6) The CP/CPS documents should be structured as defined in RFC 3647.

Evidence		Method	Rating & comment
Sections in 2527	1.1	Does the CP/CPS describe that the CP/CPS is structured as defined in RFC 3647?	C Based on RFC 2527
Sections in 3647	1.1		
CP/CPS		Is the CP/CPS structured as defined in RFC 3647?	No Based on RFC 2527

Additionally the structure is not equivalent to the structure like stated from Yoshio in his document (~ RFC 2527). This results in many „B“ - minor changes which are more or less all Policy related.

=> our practice is better than the policy

=> a lot of policy work has to be done

=> is a change to RFC 3647 recommended?

C - major changes in CA certificate

(24) The profile of the CA certificates must also comply with the current IGTF and OGF certificate profile guidelines before being included in any distribution of certificates.

Evidence		Method	Rating & comment
Sections in 2527	7.1	Check the profile of the CA certificate (details are described in the OGF Grid Certificate Profile Document).	C (or D ?) nsPolicyURL, nsBaseURL, nsRevocationURL present
Sections in 3647	7.1		
CA certificate		Check profile of the CA certificate (details should be descrbied in the OGF Grid Certificate Profile document).	nsPolicyURL, nsBaseURL, nsRevocationURL present see Attachment 1

- Also der CRL distribution point points to .pem (not .der) (– but the website delivers .der, EE certificates ok)
- Until now this hasn't broken anything – is it needed to be changed?

C - major changes in CRL

(34) The profile of the CRL must also comply with the current IGTF and OGF certificate profile guidelines[1] before being included in any distribution of certificates.

Evidence		Method	Rating & comment
Sections in 2527	7.2	Is the profile of the CRL compliant with the current IGTF and OGF certificate profile?	C should be changed to version 2 IGTF -> RFC 5280 OGF does not mention crl's
Sections in 3647	7.2		
Issued CRL		Is the profile of the CRL compliant with the current IGTF and OGF certificate profile?	v1 <-> v2

(35) The CRLs must be compliant with RFC3280, and is recommended to be version 2.

Evidence		Method	Rating & comment
Sections in 2527	7.2.1	Is the CRL compliant with RFC 3280? What is the version of the CRL?	C recommended version 2 issued version 1
Sections in 3647	7.2.1		
Issued CRL		Is the CRL compliant with RFC 3280? What is the version of the CRL?	Yes and No Version 1 (0x0) Signature Algorithm: sha1WithRSAEncryption Issuer: /C=DE/O=GermanGrid/CN=GridKa-CA Last Update: Jan 8 14:43:23 2009 GMT Next Update: Feb 7 14:43:23 2009 GMT

- version will be changed
- any known problems with crl version 2?

C - major change in EE certificates

(44) The profile of the end entity certificates must also comply with the current IGTF and OGF certificate profile guidelines before being included in any distribution of certificates.

Evidence		Method	Rating & comment
Sections in 2527	7.1	Check the profile of the EE certificates (details are described in the OGF Grid Certificate Profile Document).	C (or D ?) extendedKeyUsage not used, nsCertType used, non-repudiation included (changed in v1.6)
Sections in 3647	7.1		
Certificate Profile (if there is a separate document)		Check the profile of the EE certificates (details are described in the OGF Grid Certificate Profile Document).	see Attachement 1
End entity certificates		Check the profile of the EE certificates (details are described in the OGF Grid Certificate Profile Document).	nsPolicyURL, nsBaseURL, nsRevocationURL, ncCertType used, non-repudiation included (changed in v1.6 not approved yet)

- will be changed in version 1.6
- what about 'objsign'?

D - must be changed - EE certificates

(39) No user certificates may be shared.

Evidence		Method	Rating & comment
Sections in 2527	2.1.3	Is this described as an end-entity obligation?	D Not stated, add in CP/S
Sections in 3647	4.5.1		

(40) Each host certificate must be linked to a single network entity.

Evidence		Method	Rating & comment
Sections in 2527	3.1.2	Does the CP/CPS describe how each host certificate is linked to a single network entity?	D Not stated, add in CP/S
Sections in 3647	3.1.2, 3.1.3		
Host certificate		Does the subject name represent a single network entity?	IP-address is checked, sometimes aliases are used...

- mainly Policy work
- and to add on website with information for users

D - must be changed - Records archival

(50) These records must be available to external auditors in the course of their work as auditor.
Can be covered by auditing item (46).

Inspection	Archived logs	-Logs, certifcates, requests,crl's collected on CA-machine (2 partitions on disk, rsync to second partition, whole system 2 disks Raid 1 (mirror),); Backup on disc/usb from time to time -all checked ok -crl's detected failure in 'new' script: variable DATUM not defined, between 3/2008 and 12/2008 about a third crl's are lost :(- Requests for revocation archived as email or on webinterface/CA-DB (daily TSM-Backup – checked ok, monthly archive)

- Done

D - must be changed - Audits

(53) Every CA must perform operational audits of the CA/RA staff at least once per year.

Evidence		Method	Rating & comment
Sections in 2527	4.5	How does the CA perform operational audits?	D - audited events - audit logs analyzed once a month - keep audit logs for 3 years (ok) - CA-personnel only, copy to offline medium
Sections in 3647	5.4		
Operational manual		How does the CA perform operational audits?	not described nowhere
Interview		Ask CA operators the details of operational audit.	done last year to seldom

- RA information is verified more than once a year
- Other stuff has to be improved

D - must be changed - Publication and repository obligations

(60) The CA shall provide their trust anchor to a trust anchor repository, specified by the accrediting PMA, via the method specified in the policy of the trust anchor repository.

Evidence	Method	Rating & comment
Trust anchor repository	Does the CA provide their trust anchor?	C/D no reference to TERENA, IGTF

- Policy work only
- Practice ok, root certificate is at Terena, is in IGTF distribution

D - must be changed - Disaster recovery

(62) The CA must have an adequate compromise and disaster recovery procedure, and we willing to discuss this procedure in the PMA. The procedure need not be disclosed in the policy and practice statements.

Evidence		Method	Rating & comment
Sections in 2527	4.8	How are procedures of compromise and disaster recovery described?	D only CA priv.key compromise mentioned
Sections in 3647	5.7, 5.7.1		
Interview		Ask CA operators the detailed procedures of compromise and disaster recovery.	For all 3 machines in case of compromise: notify IGTF/OSCT/CSIRT-List, do forensics, detect what has happened, decide case, reinstall machines asap (from clean backup if possible or fresh); case CA-key compromise remove from IGTF-CA-rpm, CSIRT mail to all sites, remove crl from website (production will stumble for EE certs), create new key asap But not described nowhere

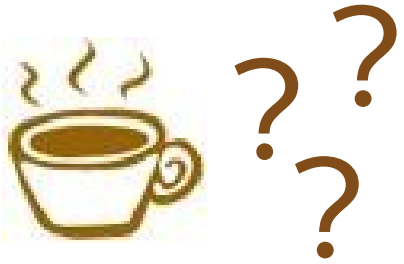
- Policy and operational manual has to be improved

Conclusion

- Find two external reviewers (Done)
- Compare rating

- Work on Policy – change to new standard (?)
- Reissue CA-certificate (??????)
- Change Extensions in EE certifcates
- Change CRL version to v.2

Karlsruhe Institute of Technology



Thank you for your attention!

Steinbuch Centre for Computing (SCC)

Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft

Universität Karlsruhe (TH)
Forschungsuniversität • gegründet 1825

Links

- http://grid.fzk.de
- https://gridka-ca-sec.fzk.de