

IGTF Audit Guidelines and GridKa-CA Self Review

Ursula Epting

STEINBUCH CENTRE FOR COMPUTING - SCC

What?

Part I General Excel-Sheet for Audits

Part II Self-Review of GridKa-CA

Part I General excel-sheet for Audits (1)

What we did:

- Took version GWD-I/CAOPs-WG - Guidelines for auditing Grid Cas version 1.1 from October 27, 2010 - copy excel
- Copied new text from:
 - IGTF PKI Technology Guidelines Version 1.0-2016 (PKITech)
 - IGTF Levels of Authentication Assurance Version 1.0-2016 (AuthAssur)to the relevant sections
- Added reference number where text is taken from
- Rephrased the questions to fit to the current text

Part I General excel-sheet for Audits (2)

3.1. Certification Authority

3.1.1. CP/CPS

(3) The CA must assign a globally unique object identifier (OID) to the CP and CPS documents		PKITech 4.3		
Evidence		Method		
Sections in 2527	1.2			
		Is OID assigned to the CP/CPS?		
Sections in 3647	1.2			
End entity certificate		Does EE cert. have PolicyID v3 extension which is set to an OID?		
OID registry (e.g. IANA)		Is OID correct?		

Part I General excel-sheet for Audits (3)

- We did not change the structure or sections reference

3.1. Certification Authority

3.1.1. CP/CPS

(1) Every CA must have a CP and CPS documents	PKITech 4.3			
Evidence	Method			
CP/CPS	Trivial			

(2) Is there a single CA organisation per country, large region or international organization?	not applicable any more?			
Evidence	Method			
Sections in 2527	1.3.1	Is there a single CA organisation per country, large region or international organization?		
Sections in 3647	1.3.1			

But we marked parts when they are not applicable anymore or are obsolete

Part I General excel-sheet for Audits (4)

Left to do by people from the community ;)

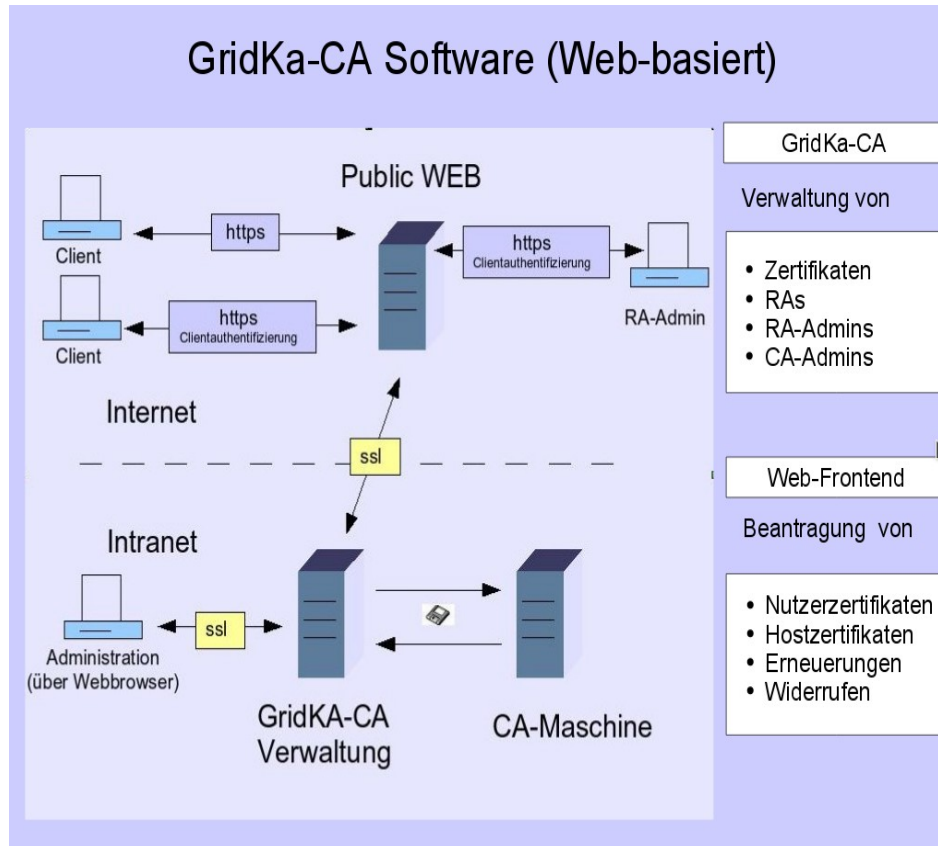
- Check if parts we marked as obsolete are obsolete
- Adapt and rename structure to fit to new structure in PKITech and AuthAssur documents – for the excel sheet AND ,Guidelines for auditing Grid Cas version
- Reorder sections in both docs
- Search for audit-worth pieces in the two docs which are not covered now

Part II Self-Review of GridKa-CA (1)

GridKa-CA is a CA run by Steinbuch Centre for Computing at Karlsruhe Institute of Technology in Germany

- Issued certificates since 2001: ~30.000
- Currently valid: ~2.200
- CA-Administrators: 3
(Ingrid Schaeffner, Melanie Ernst, me)
- Aktive RA's (~OU's): 49
- RA-admins (people): 58

Part II Self-Review of GridKa-CA (2)



- Classical offline CA, CEDAR
- Own webbased software
- Pure openssl CA with scripts

Part II Self-Review of GridKa-CA (2)

- Luckily we could rate a lot of A's
- Talking here about the others – some B's, $\frac{1}{2}$ C, 1 D and 1 X

(look at excel-sheet directly)

The end

Thank you