APGrid PMA meeting
Oct 12, 2010

NAREGI CA
Updates and Self Audit Report

Kento Aida

NAREGI CA/NII

Overview

- The operation started in 2006 (expires in 2016).
  - CP/CPS 4.4 (Classic CA Profile)
- issued certificates (9/17/2010)
  - #user certificates = 342 (19)
  - #host certificates = 2673 (174)

(): #valid ceritificates

- system
  - RA server and CA server
    - ✓ The RA server and the CA server are connected through a dedicated network
  - NAREGI-CA 2.2

Organization

- NAREGI CA
  - security officer (1), CA operator (1), RA operators (2), log administrators (2)
  - helpdesk staff (4)
- NII LRA
  - LRA administrators(2)
  - LRA operators (>20) -> distributed over 10 sites

Self Audit

- referred documents
  - Guidelines for auditing Grid CAs version 1.0
  - CP/CPS 4.4
  - the CA repository (https://www.naregi.org/ca)
  - other operational manuals
- Summary

  A: 54 B: 3 C: 8 D: 1 X: 2

Certificate Authority

1. CP/CPS

(2) Is there a single CA organisation per country, large region or international organization?

Evidence		Method	Score	Comment
Sections in 2527	1.3.1	Is there a single CA organisation per country, large region or international organization?	X	There are three CAs in Japan, AIST, KEK and NAREGI.
Sections in 3647	1.3.1			
Inspection		Is there a single CA organisation per country, large region or international organization?	X	ditto

Certificate Authority

1. CP/CPS

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

Evidence		Method	Score	Comment
Sections in 2527	1.1	Does the CP/CPS describe that the CP/CPS is structured as defined in RFC 3647?	C	We plan to change the structure following RFC3647 in the next major revision.
Sections in 3647	1.1			
CP/CPS		Is the CP/CPS structured as defined in RFC 3647?	C	ditto

Certificate Authority

3. CA Key

(17) When the CA’s cryptographic data needs to be changed, such a transition shall be managed; from the time of distribution of the new cryptographic data, only the new key will be used for certificate signing purposes.

Evidence		Method	Score	Comment
Sections in 2527	3.2, 4.7	How does the CPS describe transition of the CA’s cryptographic data?	A	
Sections in 3647	3.3.1, 4.6, 4.7, 5.6			
End entity certificates (if there was a transition of the CA’s cryptographic data)		Is the new EE cert. signed by the new cryptographic data?	X	No transition of the CA's cryptographic data.

Certificate Authority

3. CA Key

(18) The overlap of the old and new key must be at least the longest time an end-entity certificate can be valid. The older but still valid certificate must be available to verify old signatures – and the secret key to sign CRLs – until all the certificates signed using the associated private key have also expired.

Evidence		Method	Score	Comment
Sections in 2527	3.2, 4.4.7	How does the CPS describe transition of the CA's cryptographic data?	A	
Sections in 3647	3.3.1, 4.6, 4.7, 5.6			
End entity certificates Older CA certificate and private key (if there was a transition of the CA's cryptographic data)		Are new EE certificates signed by a new cryptographic data? Is the old but still valid certificate available if there are still valid certificates signed by the old private key?	X	No transition of the CA's cryptographic data.

Certificate Authority

5. Certificate Revocation

(26)Revocation requests must be properly authenticated.

Evidence		Method	Score	Comment
Sections in 2527	4.4.3	How is a revocation request authenticated?	A	
Sections in 3647	4.9.3			
Interview		Ask for details of the revocation process.	B	The description of the detailed process is missing in the operational manual. We will revise the operational manual.

Certificate Authority

6. Certificate Revocation List (CRL)

(30) Every CA must issue a new CRL immediately after a revocation.

Evidence		Method	Score	Comment
Sections in 2527	4.4.9	Is a new CRL issued immediately after a revocation?	A	CA will issue a new CRL and publish it in the repository at fixed intervals in addition to when revoking a certificate.
Sections in 3647	4.9.9			
Interview		How does the CA issue a CRL if it receives multiple revocation requests simultaneously?	B	If the CA operator receives multiple revocation requests at the same time, the CA operator issue one new CRL that includes all invocation information. This procedure is not written in the operational manual, thus, we will add the procedure in the operational manual.
Issued CRLs		Check an issued CRL to confirm that a CRL issued immediately after a revocation.	D	We found a delay (<24hrs) to issue a CRL in the log. We are now investigating the system.

Certificate Authority

6. Certificate Revocation List (CRL)

(32) The CRLs must be compliant with RFC5280.

Evidence		Method	Score	Comment
Sections in 2527	7.2.1	Is the CRL compliant with RFC 5280?	B	The CP/CPS describes that the CRL is compliant with RFC3280, X509 version 2, but the issued CRL is compliant with RFC5280. We will revise the CP/CPS.
Sections in 3647	7.2.1			
Issued CRL		Is the CRL compliant with RFC 5280?	A	The issued CRL is compliant with RFC5280.

Certificate Authority

7. End Entity Certificates and keys

(36) The authority shall issue X.509 certificates to end entities based on cryptographic data generated by the applicant, or based on cryptographic data that is be held only by the applicant on a secure hardware token.

Evidence		Method	Score	Comment
Sections in 2527	4.1, 6.1.1	How is an end entity's key generated?	A	
Sections in 3647	4.1, 4.2			
Users manual		How is an end entity's key generated?	B	The users manual includes obsolete information. We will revise the users manual.
Interview		Ask CA operators to demonstrate the generation of a CSR.	A	

Certificate Authority

7. End Entity Certificates and keys

(38) The end-entity certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125. In the certificate extensions:

Evidence		Method	Score	Comment
Sections in 2527	7.1	Do the X.509 v3 extensions conform to these requirements?	A	
Sections in 3647	7.1			
Certificate Profile (if there is a separate document)		Do the X.509 v3 extensions conform these requirements?	C	The issued end-entity certificate conform these requirements, but the information in the published profile documents is obsolete. We will revise the profile documents.
End entity certificates		Do the X.509 v3 extensions conform these requirements?	A	

Certificate Authority

7. End Entity Certificates and keys

(40) Certificates (and private keys) managed in a software token should only be re-keyed, not renewed.

Evidence		Method	Score	Comment
Sections in 2527	3.2, 4.7	How are the re-key and re-new processes described?	A	
Sections in 3647				
Users manual		How are the re-key and re-new processes described?	C	The users manual does not describe the process. We will revise the users manual.

Certificate Authority

7. End Entity Certificates and keys

(41) 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).

Evidence		Method	Score	Comment
Sections in 2527	3.2, 4.7	How is the re-new process described?	X	No stipulation for hardware token.
Sections in 3647	3.3.1, 4.6, 4.7, 5.6			
Users manual		How is the re-new process described?	X	No stipulation for hardware token.

Certificate Authority

7. End Entity Certificates and keys

(42) 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.

Evidence		Method	Score	Comment
Sections in 2527	3.2, 4.7	How are the re-key and re-new processes described? Are re-verification and authentication of identity processes required for entities on or prior to 5 years from the original/initial identity authentication?	A	
Sections in 3647	3.3.1, 4.6, 4.7, 5.6			
Users manual		How are the re-key and re-new processes described? Are re-verification and authentication of identity processes required for entities on or prior to 5 years from the original/initial identity authentication?	C	The users manual does not describe the process. We will revise the users manual.

Certificate Authority

9. Audit

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

Evidence		Method	Score	Comment
Sections in 2527	4.5	How does the CA perform operational audits?	A	
Sections in 3647	5.4			
Operational manual		How does the CA perform operational audits?	C	The operational manual does not describe the process. We will revise the operational manual.
Interview		Ask CA operators the details of operational audit.	X	ditto

Registration Authority

1. Entity Identification

(3) In case of non-personal certificate requests, an RA should validate the identity and eligibility of the person in charge of the specific entities using a secure method.

Evidence		Method	Score	Comment
Sections in 2527	2.1.2, 4.1	How does an RA validate the identity of a person requesting a host/service certificate?	A	
Sections in 3647	4.1, 4.2, 4.6, 4.7			
Operational manual		How does an RA identify a person requesting a host/service certificate?	C	The operational manual does not describe the process. We will revise the operational manual.
Interview		Ask RA operators the detailed procedure of identity vetting for host/service certificate requests.	A	

Registration Authority

1. Entity Identification

(4) For host and service certificate requests, an RA should ensure that the requestor is appropriately authorized by the owner of the associated FQDN or the responsible administrator of the machine to use the FQDN identifiers asserted in the certificate.

Evidence		Method	Score	Comment
Sections in 2527	2.1.2, 4.1	How does an RA ensure that the requestor is appropriately authorized by the owner of the FQDN?	A	
Sections in 3647	4.1, 4.2, 4.6, 4.7			
Operational manual		How does an RA ensure that the requestor is appropriately authorized by the owner of the FQDN?	C	The operational manual does not describe the process. We will revise the operational manual.
Interview		Ask RA operators the detailed procedure of identity vetting.	A	

Registration Authority

2. Name Uniqueness

(6) Over the entire lifetime of the CA it must not be linked to any other entity.

Evidence		Method	Score	Comment
Sections in 2527	3.1.4	How does the CA guarantee this requirement?	A	
Sections in 3647	3.1.5			
Interview		Ask for the details of the method to guarantee this requirement.	C	The description about the process for a person with the same family and personal name is not sufficient in the operational manual. We will revise the operational manual.

Thank you.