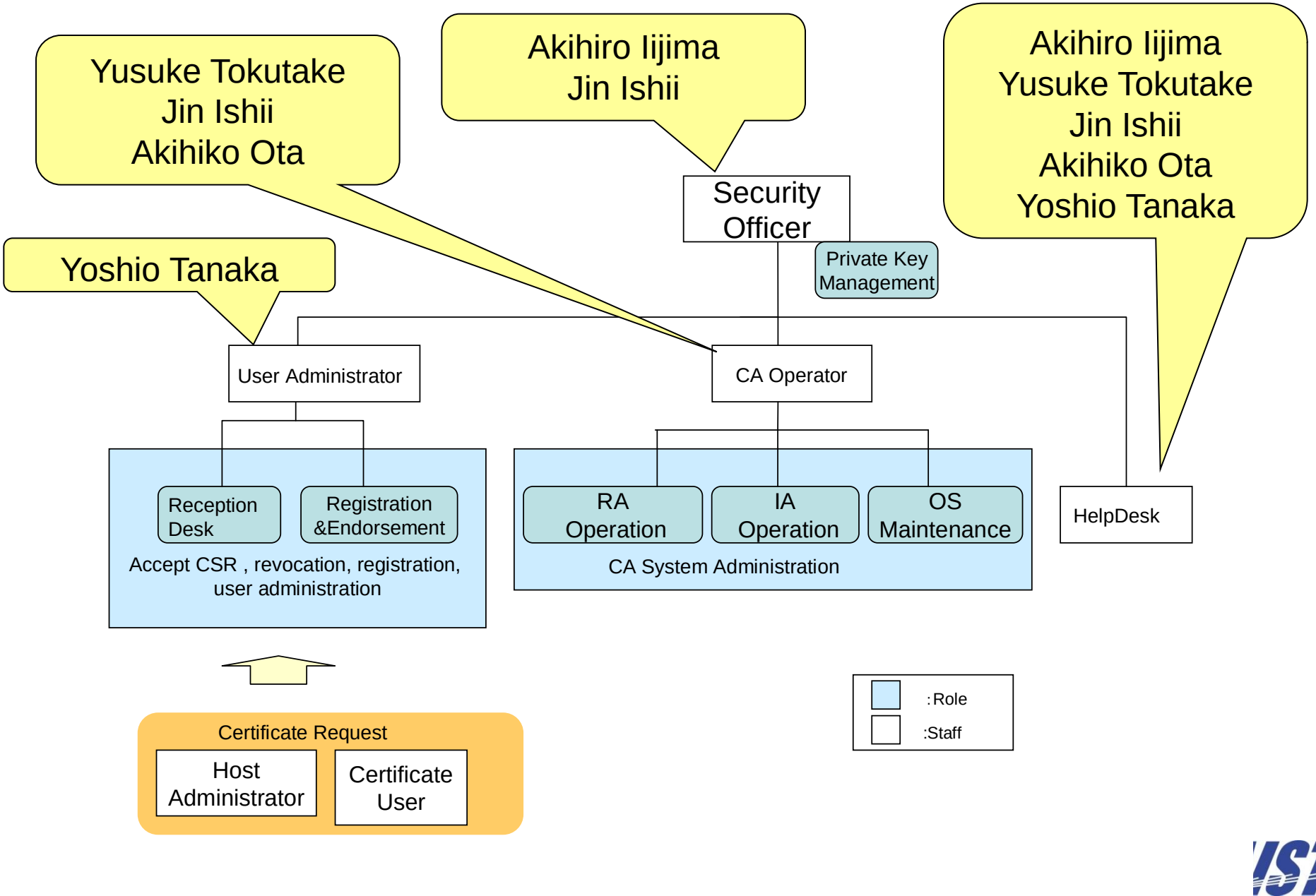
Self Audit Report of AIST GRID CA

APGridPMA Telecon
Oct 12, 2010

Yoshio Tanaka (yoshio.tanaka@aist.go.jp)
Information Technology Research Institute
AIST, Japan

Staffs


Yusuke Tokutake
Jin Ishii
Akihiko Ota
Akihiro Iijima
Jin Ishii
Akihiro Iijima
Yusuke Tokutake
Jin Ishii
Akihiko Ota
Yoshio Tanaka
Yoshio Tanaka
Security Officer
Private Key Management
User Administrator
CA Operator
Reception Desk
Registration &Endorsement
Accept CSR , revocation, registration, user administration
RA Operation
IA Operation
OS Maintenance
CA System Administration
HelpDesk
:Role
:Staff
Certificate Request
Host Administrator
Certificate User

CA Systems

- **Dedicate room**
  - Locked by card key
  - Only CA operators can enter
  - All events are recorded
- **Online CA with HSM**
  - LUNA CA3 (FIPS 140-1 Level 3)
  - CA signing server is dedicated to CA operations and connected to only RA server
- **NAREGI CA Software**

AIST

Issued certificates (updates since last VTC)

- **User certificates: 198 (188)**
  - Valid: 18 (21)
  - Invalid (revoked or expired): 180 (167)
- **Host certificates: 2494 (2464)**
  - Valid: 93 (355)
  - Invalid (revoked or expired): 2401 (2109)
- **LDAP certificates: 326 (324)**
  - Valid: 21 (22)
  - Invalid (revoked or expired): 305 (302)

Summary of self auditing

- Score A: 62
- Score B: 1
- Score C: 2
- Score D: 0
- N/A 3

Score B

(4) Whenever there is a change in the CP/CPS the O.I.D. of the document must change and the major changes must be announced to the responsible PMA and approved before signing any certificates under the new CP/CPS.

- ✓ A new OID was not assigned for editorial changes.

Score C

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

- ✓Current CPS is structured based on 2527.
- ✓Will rewrite to 3647 in the next major change.

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

- ✓Procedure is not well established.

N/A

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

- ✓ This requirement is not appropriate for AP and TAG. Discussion is still ongoing.

(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).

- ✓ Renew is not supported.

(5) An RA must validate the association of the certificate signing request.

- ✓ This is done by CA software.

AIST

Summary

- Establish a procedure of self auditing in 3 months.

Results (CA-1/14)

REQUIREMENTS	SCORE	COMMENTS
(1) Every CA must have a CP/CPS	A	
(2) Is there a single CA organisation per country, large region or international organization?	N/A	This requirement is inappropriate for some countries/regions.
(3) Every CA must assign its CP/CPS an O.I.D.	A	Obtained an OID from IANA.
(4) Whenever there is a change in the CP/CPS the O.I.D. of the document must change and the major changes must be announced to the responsible PMA and approved before signing any certificates under the new CP/CPS.	B	A new OID was not assigned for editorial changes.
(5) All the CP/CPS under which valid certificates are issued must be available on the web.	A	

Results (CA-2/14)

REQUIREMENTS	SCORE	COMMENTS
(6) The CP/CPS documents should be structured as defined in RFC 3647.	C	Current CPS is structured based on 2527.
(7) The CA computer where the signing of the certificates will take place must be a dedicated machine, running no other services than those needed for the CA signing operations.	A	
(8) The CA system must be located in a secure environment where access is controlled, limited to specific trained personnel.	A	CA system is located in a dedicated room where access is controlled.
(9) The CA system must be completely off-line or on-line. On-line CAs must use at least a FIPS 140-2 level 3 capable Hardware Security Module or equivalent and the CA system must be operated in FIPS 140-2 level 3 mode to protect the private key of CA.	A	LUNA CA3 is a FIPS 140-1 level3 capable HSM. But this is considered as FIPS 140-2 level 3 equivalent HSM.

Results (CA-3/14)

REQUIREMENTS	SCORE	COMMENTS
(10) The secure environment must be documented and approved by the PMA, and that document or an approved audit thereof must be available to the PMA.	A	
(11) The CA key must have a minimum length of 2048 bits	A	
(12) The CA key must be configured for long term use.	A	20 years
(13) If the private key of the CA is software-based, it must be protected with a pass phrase of at least 15 elements and it must be known only to designated personnel of the CA. On-line CAs using an HSM must adopt a similar or better level of security.	A	HSM is protected by a combination of physical key and pass code, which is more secure than a pass phrase.

Results (CA-4/14)

REQUIREMENTS	SCORE	COMMENTS
(14) Copies of the encrypted private key must be kept on offline media in a secure location where access is controlled.	A	Copies of the encrypted private key is in PCMCIA card which is located in a safe box.
(15) The pass phrase of the encrypted private key must also be kept on offline media, separated from the encrypted private keys and guarded in a secure location where only the authorized personnel of the CA have access. Alternatively, another documented procedure that is equally secure may be used.	A	Pass code of HSM is kept in offline media and stored in my desk with lock.
(16) The on-line CA architecture should provide for a (preferably tamper-protected) log of issued certificates and signed revocation lists.	A	

Results (CA-5/14)

REQUIREMENTS	SCORE	COMMENTS
(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.	A	
(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.	A	
(19) CA must provide and allow distribution of an X.509 certificate to enable validation of end-entity certificates.	A	

Results (CA-6/14)

REQUIREMENTS	SCORE	COMMENTS
(20) Lifetime of the CA certificate must be no longer than 20 years.	A	20 years
(21) Lifetime of the CA certificate must be no less than two times of the maximum life time of an end entity certificate.	A	
(22) The profile of the CA certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.	A	Checked all extensions.
(23) Certificate revocation can be requested by end-entities, registration authorities, and the CA. Others can request revocation if they can sufficiently prove compromise or exposure of the associated private key.	A	
(24) The CA must react as soon as possible, but within one working day, to any revocation request received.	A	

Results (CA-7/14)

REQUIREMENTS	SCORE	COMMENTS
(25) Subscribers must request revocation of its certificate as soon as possible, but within one working day after detection of - he/she lost or compromised the private key pertaining to the certificate, - the data in the certificate are no longer valid.	A	
(26) Revocation requests must be properly authenticated.	A	A user who has a valid private key can revoke immediately.
(27) Every CA must generate and publish CRLs.	A	
(28) The CRL lifetime must be no more than 30 days.	A	
(29) Every CA must issue a new CRL at least 7 days before the time stated in the nextUpdate field for off-line CAs, at least 3 days before the time stated in the nextUpdate field for automatically issued CRLs by on-line CAs.	A	

Results (CA-8/14)

REQUIREMENTS	SCORE	COMMENTS
(30) Every CA must issue a new CRL immediately after a revocation.	A	
(31) The signed CRL must be published in a repository at least accessible via the World Wide Web, as soon as issued.	A	
(32) The CRLs must be compliant with RFC5280.	A	
(33) The user key and the host key must have a minimum length of 1024 bits.	A	
(34) Lifetime of user certificates and host certificates must be no longer than 13 months.	A	12 months
(35) No user certificates may be shared.	A	

Results (CA-9/14)

REQUIREMENTS	SCORE	COMMENTS
(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.	A	A key pair is generated on the client machine.
(37) Every CA should make a reasonable effort to make sure that subscribers realize the importance of properly protecting their private data. When using software tokens, the private key must be protected with a strong pass phrase, i.e., at least 12 characters long and following current best practice in choosing high-quality passwords. Private keys pertaining to host and service certificate may be stored without a passphrase, but may be adequately protected by system methods.	A	

Results (CA-10/14)

REQUIREMENTS	SCORE	COMMENTS
(38) The end-entity certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.	A	Checked all extensions.
(39) If a commonName component is used as part of the subject DN, it should contain an appropriate presentation of the actual name of the end-entity.	A	Checked manually.
(40) Certificates (and private keys) managed in a software token should only be re-keyed, not renewed.	A	
(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).	N/A	

Results (CA-11/14)

REQUIREMENTS	SCORE	COMMENTS
(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.	A	
(43) 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.	A	
(44) These records must be available to external auditors in the course of their work as auditor.	A	

Results (CA-12/14)

REQUIREMENTS	SCORE	COMMENTS
(45) These records must be kept for at least three years, where the identity validation records must be kept at least as long as there are valid certificates based on such a validation.	A	
(46) Each CA must accept being audited by other accredited CAs to verify its compliance with the rules and procedures specified in its CP/CPS document.	A	
(47) Every CA should perform operational audits of the CA/RA staff at least once per year.	C	Procedure is not well established.
(48) A list of CA and RA personnel should be maintained and verified at least once per year.	A	
(49) The repository must be run at least on a best-effort basis, with an intended availability of 24x7.	A	

Results (CA-13/14)

REQUIREMENTS	SCORE	COMMENTS
(50) The accredited authority must publish their X.509 signing certificate as the root of trust.	A	
(51) Each authority must publish the following for their subscribers, relying parties and for the benefit of distribution by the PMA and the federation	A	
(52) The originating authority must grant to the PMA and the Federation – by virtue of its accreditation – the right of unlimited re-distribution of this information.	A	
(53) The CA should provide a means to validate the integrity of its root of trust.	A	
(54) 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.	A	

Results (CA-14/14)

REQUIREMENTS	SCORE	COMMENTS
(55) Accredited CAs must define a privacy and data release policy compliant with the relevant national legislation. The CA is responsible for recording, at the time of validation, sufficient information regarding the subscribers to identify the subscriber. The CA is not required to release such information unless provided by a valid legal request according to national laws applicable to that CA.	A	
(56) 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.	A	

Results (RA-1/3)

REQUIREMENTS	SCORE	COMMENTS
(1) A PKI CA must define the role of a registration authority (RA), and these RAs are responsible for the identity vetting of all end entities.	A	
(2) In order for an RA to validate the identity of a person, the subject should contact the RA face-to-face and present photo-id and/or valid official documents showing that the subject is an acceptable end entity as defined in the CP/CPS document of the CA.	A	
(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.	A	

Results (RA-2/3)

REQUIREMENTS	SCORE	COMMENTS
(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.	A	
(5) An RA must validate the association of the certificate signing request.	N/A	This is done by CA software.
(6) The CA or RA should have documented evidence on retaining the same identity over time. In all cases, the certificate request submitted for certification must be bound to the act of identity vetting.	A	
(7) Any single subject distinguished name must be linked to one and only one entity.	A	
(8) Over the entire lifetime of the CA it must not be linked to any other entity.	A	

Results (RA-3/3)

REQUIREMENTS	SCORE	COMMENTS
(9) All communications between the CA and the RA regarding certificate issurance or changes in the status of a certificate must be by secure and auditable methods.	A	Use signed email.
(10) The CP/CPS should describe how the RA or CA is informed of changes that may affect the status of the certificate.	A	
(11) The RA must record and archive all requests and confirmations.	A	
(12) The CA is responsible for maintaining an archive of these records in an auditable form.	A	