GFD-I.169
Category: Informational
CAOPs-WG

Y Tanaka, M Viljoen, S Rea

April 19, 2010

Guidelines for auditing Grid CAs version 1.0

Status of This Memo

This memo provides information to the Grid community on the guidelines for auditing Grid CAs. It does not define any standards or technical recommendations. Distribution is unlimited.

Abstract

Grids use X.509 certificates for authentication and authorization. These certificates are issued to subscribers that comprise a virtual organization, and are typically issued by Certification Authorities operated by real institutions. In order to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures, these Certification Authorities (CAs) should be externally audited periodically. The International Grid Trust Federation (IGTF) has, based on templates established by OGF, established such sets of operational policies and procedures. This document provides an audit checklist which describes auditing items to be considered by CAs accredited by the IGTF to be compliant with the 'Classic' Authentication Profile, and provides the acceptable evidence for the verification of these items. Detailed processes of auditing are also described in this document which is intended as guidelines for auditing Grid CAs. Spread sheets of the check list for 'Classic', 'Short Lived Credential Services (SLCS)', and 'Member Integrated Credential Services (MICS)' profiles are provided as separate documents and available on the IGTF web site. This document as well as the spread sheets will be maintained and updated when there is a newer version of authentication profiles available than it refers.

1. Introduction

Grids use X.509 certificates for authentication and authorization. Those certificates are typically issued by Certification Authorities (CAs) operated by real institutions whose subscribers comprise a virtual organization. In order to ensure compliance with the policies and operational procedures, such as those established by the International Grid Trust Federation (IGTF), and to recommend necessary changes in controls, policies or procedures, these CAs should be externally audited on a periodic basis. Processes of auditing include an independent examination of documentation, records, and observed activities to assess the adequacy of system controls. Auditing processes generally also require the interviewing of the staff responsible for administration and operation of the CA, and the inspection of evidence and physical devices, etc that comprise the CA infrastructure. The audit checklist below (see Section 3), is built based upon the IGTF *Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure* Version 4.2. This document provides the audit checklist which describes auditing items and evidences for their verification. Detailed processes of auditing are also described in this document which is intended as guidelines for auditing IGTF accredited Grid CAs. Spread sheets of the check list for 'Classic', 'Short Lived Credential Services (SLCS)', and 'Member Integrated Credential Services (MICS)' profiles are provided as separate documents and available on the IGTF web site. This document as well as the spread sheets will be maintained and updated when there is a newer version of authentication profiles available than it refers.

The purpose of this paper is to show guidelines for auditing IGTF accredited Grid CAs and does NOT imply that the OGF accepts any responsibility and liability resulting from reliance on such audits.

2. Procedures of auditing

2.1. Auditing Scoring

Auditors prepare an audit rating, which is a tabulation of the audit checklist, evidence, procedures and results of the examination, and scores of the individual items in the audit checklist. Each item in the audit checklist should be scored according to the results of the examination. For example, each item can be scored from A to D, and X as below.

- A: Good.
- B: Recommendation (minor change)
- C: Recommendation (major change)
- D: Advice (must change)
- X: Could not evaluate (N/A)

2.2. Auditing process

Auditing consists of a 3-step examination process – a pre-examination, a main examination, and a post examination. The pre-examination collates and reviews the relevant documentation, the main examination observes the operational practices, and the post-examination is to verify the resulting audit report. Each of the activities for these examination processes is detailed below.

2.3. Pre-Examination

In the pre-examination, all possible documents available for the auditors are examined. The followings are examples of such documents.

- CP/CPS
- Relevant IGTF Authentication Profile(s)
- Manuals for subscribers (e.g. enrollment manual)
- Operational manuals (for CA and/or RA operators)
- CA Repository (e.g. Web site)
- CA Certificate
- CRL
- End entity certificates (subscribers, CA and/or RA operators)
- HSM manual (or appropriate web site)
- Any other document described as “published in the repository” in the CP/CPS
- Any other document available for the auditors

Some of these documents must be available in the repository and the auditors can request that the CA provide the other documents.

In the pre-examination, the auditors evaluate each item in the audit checklist by examining all appropriate available documentation. Some of the checklist items could be scored according to the results of the pre-examination, but other items may need an interview with the CA operators and physical inspections in order to be scored. Necessary evidences for the evaluation depend on available materials and their usefulness for the pre-examination. If the auditors are unable to score an item, the auditors should describe necessary examinations, interviews, and inspections in the audit rating table, which will be carried out during the main examination.

2.4. Main examination

In the main examination, the auditors visit the CA, interview the CA staff, and inspect documents (e.g. archived logs) and equipment (e.g. CA server, HSM, backup media, etc) according to the results of the pre-examination. The auditors should score the items which could not be scored in the pre-examination.

In this examination stage, the auditors visit the CA and interview the staff responsible for the administration and operation of the CA, and inspect evidence and physical devices, etc, and observe operations. The followings are examples of items that may be inspected.

- CA room
- CA machine including HSM and its activation
- A backup media of the CA private key and its place (e.g. a safe box).
- Offline media (e.g. a sealed envelope) which contains a pass phrase of the CA private key and its place (e.g. a safe box).

- Media storage of archived logs and other documents and their place (e.g. a safe box).
- End entity certificates (if not available for the pre-examination), including issuance activities
- Logs of the CA/RA servers
- Logs of the CA repository (e.g. Web server)
- Records of operation of the CA private key (including accesses to the HSM)
- Access log to the CA room
- Any other documents (e.g. daily report of the CA operators)

2.5. Post-Examination

In the post-examination, the auditors draft an auditing report according to the results of the pre-examination and the main examination. The audit report should include the followings:

- Date of auditing
- Terms of subjects of auditing
- Names of the auditors
- Names of the participants
- Results of the auditing
  - Scores of the items in the audit checklist
  - Comments for Scores B, C, and D.

The auditing report should be drafted and sent to the CA within few days after the auditing. A copy of the audit report may also be forwarded to the relevant IGTF PMA. The CA is expected to send a report on the plans for improving the CA operation to the auditors and the relevant IGTF PMA within a few weeks.

2.6. Auditing Scoring

The audit/assessment/evaluation team and the individuals on that team, should be qualified to assess the policies and practices of a PKI. Auditors should be competent to evaluate the CA management processes and operational procedures, its related IT security components and its PKI-unique elements. A PKI audit team shall consist of individuals who together have the necessary skills and experience to assess the policies, procedures and practices of the PKI. External auditors should be individually and organizationally independent of the PKI that is being audited, internal auditors should at least be individually independent of the PKI that is being audited.

The specific auditor qualification requirements are that they should be competent, independent, understand PKIs, understand auditing methods, and understand IGTF profiles. The following is a list of considerations to undertake when determining the expertise and qualifications of members of the assessment team carrying out a PKI audit (NOTE: These considerations are provided simply in an advisory capacity and not as hard requirements when determining auditor qualifications):

- Professional Certifications such as CISSP and CISA or equivalent;
- Successful completion of training courses in assessment of IT security controls;
- Knowledge of one or more Structured and documented Systems Security methodologies;
- Knowledge of how to perform an IT Operational Audit;
- Three years of recent PKI experience;
- Knowledge of how to interpret Certificate Policy (CP) and Certification Practice Statement (CPS);
- Understanding of RFC 3647 framework for defining CP and CPS;
- Understanding and familiarity with the IGTF Classic Authentication Profile V 4.1
- Understanding of the relation between the framework, CP, CPS and PKI Operations;
- Understanding of the function of the CPS;
- Knowledge of the components of a PKI and their functions;
- Demonstrable previous audit experience;
- Experience in information systems risk analysis.

3. Auditing Checklist

This section shows an auditing checklist. For each item, evidence and methods for the evaluation such as the section number of the CP/CPS, subjects of the inspections and issues to be interviewed, are described. The indicated section numbers of the CP/CPS are according to RFC3647 (NOTE: RFC2527 references are also included for legacy purposes, but CAs operating in compliance with the

IGTF Classic CA Authentication Profile Version 4.1 should have their CP/CPS formatted according to RFC3647). Sections shown as evidences may vary.

3.1. Certification Authority

3.1.1. CP/CPS

(1) Every CA must have a CP/CPS

Evidence	Method
CP/CPS	Trivial

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

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	
Inspection		Is there a single CA organisation per country, large region or international organization?

(3) Every CA must assign its CP/CPS an O.I.D.

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?

(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.

Evidence		Method
Sections in 2527	8.1	Does the CP/CPS describe the CP/CPS change procedures, publication and notification policies, and approval procedures?
Sections in 3647	9.12	
Interview		Ask for details of the CP/CPS administration. For example, who makes changes and who makes decision (approval)?

(5) All the CP/CPS under which valid certificates are issued must be available on the web.

Evidence		Method
Sections in 2527	2.6.1	Does the CP/CPS describe that all the CP/CPSes under which valid certificates are issued are available on the web?
Sections in 3647	2.2, 4.4.2, 4.4.3, 4.6.6, 4.6.7, 4.7.6, 4.7.7, 4.8.6, 4.8.7	
Web repository		Are all the CP/CPSes available on the web?

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

Evidence		Method
Sections in 2527	1.1	Does the CP/CPS describe that the CP/CPS is structured as defined in RFC 3647?
Sections in 3647	1.1	
CP/CPS		Is the CP/CPS structured as defined in RFC 3647?

3.1.2. CA System

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.

Evidence		Method
Sections in 2527	6.5.1	Is the CA system a dedicated machine?
Sections in 3647	6.5.1	
Inspection		CA system

(7) The CA system must be located in a secure environment where access is controlled, limited to specific trained personnel.

Evidence		Method
Sections in 2527	5.1.1, 5.1.2	Is the CA system located in a secure environment where access is controlled?
Sections in 3647	5.1.1, 5.1.2	
Interview		Ask for details of access control to the CA system and its location. For example, who can access to the CA system? How is the access controlled? Is a single person allowed to access to the CA system? How is the access log recorded?
Inspection		Location of the CA system

(8) 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.

Evidence		Method
Sections in 2527	6.1.8, 6.2.1, 6.7	Is the CA system completely off-line or one-line which uses FIPS 140-2 level 3 capable HSM operated in FIPS 140-2 level 3 mode?
Sections in 3647	6.1.1, 6.2.1, 6.7	
HSM manual		Is the HSM at least FIPS 140-2 level 3?
Inspection		CA system

(9) 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.
Can be covered by the auditing item (7).

3.1.3. CA Key

(10) The CA key must have a minimum length of 2048 bits

Evidence		Method
Sections in 2527	6.1.5	Is the CA key length 2048 bit?
Sections in 3647	6.1.5	
Certificate Profile		Is the CA key length 2048 bit?
CA Certificate		Is the CA key length 2048 bit?

(11) The CA key must be configured for long term use

Evidence		Method
Sections in 2527	6.3.2	Is the CA key configured for long term use?
Sections in 3647	6.3.2	
CA Certificate		Is the CA key regenerated when the CA certificate is rolled over? If so is rollover configured to occur at a sufficiently sparse time period? NOTE: If the CA key is stored in software it must only be re-keyed at rollover – see item (46) below

(12) 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.

Evidence	Method

Sections in 2527	6.2.7	Does the CPS describe the protection of the CA private key?
Sections in 3647	6.2.8	
Interview		Ask CA operators who knows the pass phrase. Recommend that CA operators implement multi-person control.

(13) Copies of the encrypted private key must be kept on offline media in a secure location where access is controlled.

Evidence		Method
Sections in 2527	6.2.4	Is the CA private key backup in offline medium?
Sections in 3647	6.2.4	
Inspection		Backup media and location.

(14) 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.

Evidence		Method
Sections in 2527	6.2.4, 6.2.5	Is the pass phrase of CA private key kept in offline medium?
Sections in 3647	6.2.4, 6.2.5	
Inspection		Backup media and location.

(15) The on-line CA architecture should provide for a (preferably tamper-protected) log of issued certificates and signed revocation lists.

Evidence		Method
Sections in 2527	4.6.1, 4.6.3	Does the on-line CA provide a log of issued certificates and a signed revocation list? Is the log tamper-protected?
Sections in 3647	5.5.1, 5.5.3	
Inspection		Log of issued certificates and signed revocation list.

(16) 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
Sections in 2527	3.2, 4.7	How does the CPS describe transition of the CA's cryptographic data?
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?

(17) 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
Sections in 2527	3.2, 4.4.7	How does the CPS describe transition of the CA's cryptographic data?
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?

3.1.4. CA Certificate

(18) CA must provide and allow distribution of an X.509 certificate to enable validation of end-entity certificates.

Evidence		Method
Sections in 2527	2.6.1, 8.2	Is the CA certificate X.509 compliant and published to a repository?
Sections in 3647	2.2	
CA certificate		Check that the CA certificate is X.509 V3 compliant and published to a repository.

(19) Lifetime of the CA certificate must be no longer than 20 years.

Evidence		Method
Sections in 2527	4.7	How long is the lifetime of the CA certificate?
Sections in 3647	5.6	
CA certificate		Check the lifetime of the CA certificate.

(20) Lifetime of the CA certificate must be no less than two times of the maximum life time of an end entity certificate.

Evidence		Method
Sections in 2527	4.7	How long are the lifetimes of the CA certificate and end entity certificate?
Sections in 3647	5.6	
CA certificate and end entity certificate		Check the lifetime of the CA certificate and end entity certificate.

(21) The profile of the CA certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

Evidence		Method
Sections in 2527	7.1	Check profile of the CA certificate (details are described in the OGF Grid Certificate Profile Document, GFD.125).
Sections in 3647	7.1	
CA certificate		Check profile of the CA certificate (details are descried in the OGF Grid Certificate Profile document, GFD.125).

3.1.5. Certificate Revocation

(22) 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.

Evidence		Method
Sections in 2527	4.4.2	Who can request revocation?
Sections in 3647	4.8.2, 4.9.2	

(23) The CA must react as soon as possible, but within one working day, to any revocation request received.

Evidence		Method
Sections in 2527	4.4.3	How the CA react to revocation requests?
Sections in 3647	4.9.5	

(24) 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 or the data in the certificate are no longer valid.

Evidence		Method
Sections in 2527	2.1.3, 4.4.1	Does an end entity obligation include requesting revocation if she/he lost or compromised the private key or any data in the certificate is no longer valid?
Sections in 3647	4.9.1	

(25) Revocation requests must be properly authenticated.

Evidence		Method
Sections in 2527	4.4.3	How is a revocation request authenticated?
Sections in 3647	4.9.3	

Interview	Ask for details of the revocation process.

3.1.6. Certificate Revocation List (CRL)

(26) Every CA must generate and publish CRLs.

Evidence		Method
Sections in 2527	2.1.1	Does the CA issues CRLs?
Sections in 3647	4.9.7	
Web repository		Are CRLs available on the web?

(27) The CRL lifetime must be no more than 30 days.

Evidence		Method
Sections in 2527	4.4.9	How long is the lifetime of the CRL?
Sections in 3647	4.9.9	
Issued CRLs		Is the lifetime of a CRL less than 30 days?

(28) 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.

Evidence		Method
Sections in 2527	4.4.9	Is a new CRL issued at least 7 days before expiration (for off-line) or 3 days before expiration (for on-line)?
Sections in 3647	4.9.9	
Issued CRLs		Is a CRL issued at least 7 days before expiration (for off-line) or 3 days before expiration (for on-line)?

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

Evidence		Method
Sections in 2527	4.4.9	Is a new CRL issued immediately after a revocation?
Sections in 3647	4.9.9	
Interview		How does the CA issue a CRL if it receives multiple revocation requests simultaneously?
Issued CRLs		Check an issued CRL to confirm that a CRL issued immediately after a revocation.

(30) The signed CRL must be published in a repository at least accessible via the World Wide Web, as soon as issued.
Can be covered by the auditing item (29).

(31) The CRLs must be compliant with RFC5280.

Evidence		Method
Sections in 2527	7.2.1	Is the CRL compliant with RFC 5280?
Sections in 3647	7.2.1	
Issued CRL		Is the CRL compliant with RFC 5280?

3.1.7. End Entity Certificates and Keys

(32) The user key and the host key must have a minimum length of 1024 bits.

Evidence		Method
Sections in 2527	6.1.5	Is the length of user/host keys at least 1024 bit?
Sections in 3647	6.1.5	
Certificate Profile		Is the length of user/host keys at least 1024 bit?
User and host Certificate		Is the length of user/host keys at least 1024 bit?

(33) Lifetime of user certificates and host certificates must be no longer than 13 months.

Evidence		Method
Sections in 2527	4.7	How long is the lifetime of user and a host certificates?
Sections in 3647	5.6	
CA certificate		Check the lifetime of user and host certificates.

(34) No user certificates may be shared.

Evidence		Method
Sections in 2527	2.1.3	Is this described as an end-entity obligation?
Sections in 3647	4.5.1	

(35) 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
Sections in 2527	4.1, 6.1.1	How is an end entity's key generated?
Sections in 3647	4.1, 4.2	
Users manual		How is an end entity's key generated?
Interview		Ask CA operators to demonstrate the generation of a CSR.

(36) 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.

Evidence		Method
Sections in 2527	6.2.7	Is this described as an end-entity obligation?
Sections in 3647	6.2.8	

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

i. a policyIdentifier must be included and must contain an OID identifying the CP document under which the certificate was issued, and should contain only OIDs
ii. the policyIdentifier must include the OID or Authentication Profile under which the Certification Authority has been accredited. For Classic AP, OID is 1.2.840.113612.5.2.2.1.
iii. CRLDistributionPoints must be included and contain at least one http URL.
iv. an OCSP URI may be included in the AuthorityInfoAccess extension only if the OCSP responder is operated as a production service by or on behalf of the issuing CA.

Evidence		Method
Sections in 2527	7.1	Do the X.509 v3 extensions conform to these requirements?
Sections in 3647	7.1	
Certificate Profile (if there is a separate document)		Do the X.509 v3 extensions conform these requirements?
End entity certificates		Do the X.509 v3 extensions conform these requirements?

(38) 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.

Evidence		Method
Sections in 2527	3.1.2	Does the CPS describe need for names to be meaningful?
Sections in 3647	3.1.2, 3.1.3	
End entity certificates		Check end entity certificates.

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

Evidence		Method
Sections in 2527	3.2, 4.7	How are the re-key and re-new processes

Sections in 3647		described?
Users manual		How are the re-key and re-new processes described?

(40) 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
Sections in 2527	3.2, 4.7	How is the re-new process described?
Sections in 3647	3.3.1, 4.6, 4.7, 5.6	
Users manual		How is the re-new process described?

(41) 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
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?
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?

3.1.8. Records Archival

(42) 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.

Evidence		Method
Sections in 2527	4.6.1	Does the CA record and archive all requests for certificates, along with all issued certificates, all request for revocation, all issued CRLs and login/logout/reboot information of the issuing machine?
Sections in 3647	5.5.1	
Inspection		Archived logs

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

(44) 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.

Evidence		Method
Sections in 2527	4.6.2	Is the archive kept at least three years? Is the identity validation record kept at least as long as there are valid certificates based on such a validation?
Sections in 3647	5.5.2	
Inspection		Archived logs

3.1.9. Audits

(45) 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.

Evidence		Method
Sections in 2527	2.7	Does the CA accept external auditing?

Sections in 3647	8	How is the procedure of auditing described in the CP/CPS?

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

Evidence		Method
Sections in 2527	4.5	How does the CA perform operational audits?
Sections in 3647	5.4	
Operational manual		How does the CA perform operational audits?
Interview		Ask CA operators the details of operational audit.

(47) A list of CA and RA personnel should be maintained and verified at least once per year.

Evidence	Method
A list of CA and RA personnel	Is the list appropriately maintained?

3.1.10. Publication and Repository Responsibilities

(48) The repository must be run at least on a best-effort basis, with an intended availability of 24x7.

Evidence		Method
Sections in 2527	2.6.4	Is the web repository available 24x7 on a best effort basis?
Sections in 3647	2.1	
Web repository		Is the web repository available?

(49) The accredited authority must publish their X.509 signing certificate as the root of trust.

Evidence		Method
Sections in 2527	2.6.1	Is the CA root certificate published?
Sections in 3647	2.2, 4.4.2	
Web repository		Is the CA root certificate published?

(50) Each authority must publish the following for their subscribers, relying parties and for the benefit of distribution by the PMA and the federation

i. the CA root certificate or set of CA root certificates up to a self-signed root;
ii. a http or https URL of the PEM-formatted CA certificate;
iii. a http URL of the PEM or DER formatted CRL;
iv. a http or https URL of the web page of the CA for general information;
v. the CP and/or CPS documents;
vi. an official contact email address for inquiries and fault reporting
vii. a physical or postal contact address

Evidence		Method
Sections in 2527	2.6.1	Is this information published?
Sections in 3647	2.2, 4.4.2, 4.6.6, 4.7.6, 4.8.6	
Web repository		Is this information published?

(51) 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.

Evidence	Method
Re-distribution sites	Is this information re-distributed?

(52) The CA should provide a means to validate the integrity of its root of trust.

Evidence	Method
Web repository	Does the CA provide a means to validate the integrity of its root of trust?

(53) 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
Trust anchor repository	Does the CA provide their trust anchor?

3.1.11. Privacy and Confidentiality

(54) 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.

Evidence		Method
Sections in 2527	2.8	How are privacy and confidentiality described?
Sections in 3647	9.3, 9.4	

3.1.12. Compromise and Disaster Recovery

(55) 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
Sections in 2527	4.8	How are procedures of compromise and disaster recovery described?
Sections in 3647	5.7, 5.7.1	
Interview		Ask CA operators the detailed procedures of compromise and disaster recovery.

3.2. Registration Authority

3.2.1. Entity Identification

(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.

Evidence		Method
Sections in 2527	2.1.2, 4.1	What is the role of the RA?
Sections in 3647	4.1, 4.2, 4.6, 4.7	

(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.

Evidence		Method
Sections in 2527	2.1.2, 4.1	How does an RA implement identity vetting?
Sections in 3647	4.1, 4.2, 4.6, 4.7	
Operational manual		How does an RA identify a person?
Interview		Ask RA operators the detailed procedure of identity vetting.

(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
Sections in 2527	2.1.2, 4.1	How does an RA validate the identity of a person requesting a host/service certificate?
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?
Interview		Ask RA operators the detailed procedure of identity vetting for host/service certificate requests.

(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
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?
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?
Interview	Ask RA operators the detailed procedure of identity vetting.

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

Evidence		Method
Sections in 2527	4.3	How does an RA validate the association of the certificate signing request?
Sections in 3647	4.1	
Operational manual		How does an RA validate the association of the certificate signing request?
Interview		Ask RA operators how they validate the association of the certificate signing request.

(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.

Evidence		Method
Sections in 2527	4.6.1	Does the CA or RA have documented evidence on retaining the same identity over time?
Sections in 3647	5.5.1	
Inspection		Documented evidence

3.2.2. Name Uniqueness

(5) Any single subject distinguished name must be linked to one and only one entity.

Evidence		Method
Sections in 2527	3.1.4	How does the CA guarantee the uniqueness of the subject name?
Sections in 3647	3.1.5	
Interview		How does the CA guarantee the uniqueness of the subject name? What happens if there are two persons whose names are the same in the same organization?

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

Evidence		Method
Sections in 2527	3.1.4	How does the CA guarantee this requirement?
Sections in 3647	3.1.5	
Interview		Ask for the details of the method to guarantee this requirement.

3.2.3. RA to CA Communications

(7) 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.

Evidence		Method
Sections in 2527	4.1, 4.2	How does the CA communicate with the RA?
Sections in 3647	4.1, 4.2	
Operational manual		How does CA communicate with the RA?
Interview		Ask for the details of how the CA communicates with the RA (e.g. how the CSR is sent to the CA and the signed certificate is sent to the RA).

(8) The CP/CPS should describe how the RA or CA is informed of changes that may affect the status of the certificate.

Evidence		Method
Sections in 2527	4.4	How is the CA or the RA informed of

Sections in 3647	4.8, 4.9	changes?
Interview		Ask for the details of how the CA or the RA is informed of change.

3.2.4. Records Archival

(9) The RA must record and archive all requests and confirmations.

Evidence		Method
Sections in 2527	4.6.1	Does the RA record and archive all requests and confirmations?
Sections in 3647	5.5.1	
Inspection		Archives of all requests and confirmations.

(10) The CA is responsible for maintaining an archive of these records in an auditable form.

Evidence		Method
Sections in 2527	4.6	Does the RA maintain the archive of these records in an auditable form?
Sections in 3647	5.5.1	
Inspection		Archives of these records archival.

4. Security Considerations

The IGTF defines Authentication Profiles and each member PMA is responsible for accrediting member Certificate Authorities according to a specific profile. Once a member CA is accredited by its respective PMA, it is expected to do self-auditing and/or to accept external auditing to confirm the compliance of the CA. This document describes guidelines for auditing Grid CAs which comply with the Classic Authentication Profile and the audit checklist is built based on the Classic Authentication Profile Version 4.1. Since evidences for verifying each audit item may differ between CAs, auditors must carefully verify the audit item with appropriate evidences. Auditors should especially be interested in the certificate life cycle management, protection of CA's private key, and logs are archived enough to trace anything when something would happen.

5. Contributors

This document captures the collective knowledge of many people, and the editor is grateful for the contributions made to this document by the members of the International Grid Trust Federation [IGTF], the individual certification authorities and relying parties that have conducted the experiments and tests, and the valuable contributions from the participants in the CAOPS WG.

The editors,
Yoshio Tanaka (yoshio.tanaka@aist.go.jp)
Matthew Viljoen (matt.viljoen@stfc.ac.uk)
Scott Rea (Scott.Rea@Dartmouth.EDU)

6. Intellectual Property Statement

7. Disclaimer

This document and the information contained herein is provided on an “As Is” basis and the OGF disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

8. Full Copyright Notice

9. References

[1] S. Chokhani and W. Ford, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, RFC2527, The Internet Society, 1999.
[2] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, RFC3647, The Internet Society, 2003.
[3] D. Groep, “Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure”, International Grid Trust Federation, IGTF-AP-classic-4-2, 2008.
[4] FPKIPA, HEBCA, SAFE, and CertiPath, “PKI Audit Guidelines”, Four Bridge Forum PKI Audit Working Group, Draft, 2008