AIST GRID CA Updates
audit and new CP/CPS

Yoshio Tanaka (yoshio.tanaka@aist.go.jp)
Grid Technology Research Center,
AIST, Japan
Contents

- AIST GRID CA was audited by NAREGI CA in March 29.
  - Overview of audit
  - Schedule
  - Experiences
  - Summary
- New CP/CPS
  - Version 1.1 (June 6)
  - Version 1.1.1 (June 15)
Proposed audit items

- NAREGI PKI WG has subjectively selected criteria for auditing Grid CAs.
  - based on
    - AICPA/CICA WebTrust℠/™ Program for Certification Authority
    - minimum CA requirements of APGrid PMA and EUGrid PMA

- Web Trust
  - WebTrust is a seal awarded to websites that consistently adhere to certain business standards established by the Canadian Institute of Chartered Accountants (CICA.ca) and the American Institute of Certified Public Accountants (AICPA).
  - In the program, “Web Trust Principles and Criteria for Certification Authorities” lists criteria for CAs.
  - may be too much for Grid CAs.
Criteria in the WebTrust<sup>SM/TM</sup>

**Principle 1: CA Business Practices Disclosure**
- The certification authority discloses its key and certificate life cycle management business and information privacy practices and provides its services in accordance with its disclosed practices.

**Principle 2: Service Integrity**
- The certification authority maintains effective controls to provide reasonable assurance that:
  - Subscriber information was properly authenticated (for the registration activities performed by ABC-CA) and
  - The integrity of keys and certificates it manages is established and protected throughout their life cycles.
Criteria in the WebTrust™ (cont’d)

Principle 3: CA Environmental Controls

The certification authority maintains effective controls to provide reasonable assurance that:

- Subscriber and relying party information is restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
- The continuity of key and certificate life cycle management operations is maintained; and
- CA systems development, maintenance, and operation are properly authorized and performed to maintain CA systems integrity.
Audit checklist

Simply pickup items from WebTrust™ criteria based on minimum CA requirements.

The number of criteria:

<table>
<thead>
<tr>
<th>Principle</th>
<th>WebTrust™</th>
<th>Check List</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1</td>
<td>45</td>
<td>13</td>
</tr>
<tr>
<td>Principle 2</td>
<td>188</td>
<td>14</td>
</tr>
<tr>
<td>Principle 3</td>
<td>165</td>
<td>7</td>
</tr>
<tr>
<td>Others</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>
Experiences on being audited

- AIST GRID CA was audited by NAREGI CA according to the proposed criteria for audit.

Term of auditing
- Preliminary examination: Feb. 21 ~ Mar. 28
- Main examination: Mar. 29

Auditors
- Three auditors from NEC/NAREGI.
- Chief auditor is an expert of auditing

Procedure
- Examination of documents
- Interview to Security Officers, CA operators, and User Administrators
- Inspection of the CA server room, CA system (including HSM), and a safe box
# Subjects of auditing

<table>
<thead>
<tr>
<th>No</th>
<th>Subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Documents</strong></td>
</tr>
<tr>
<td>2</td>
<td>Certificate and CRL Profile</td>
</tr>
<tr>
<td>3</td>
<td>AIST GRID CA Enrollment Procedure Document</td>
</tr>
<tr>
<td>4</td>
<td>Operation Manual</td>
</tr>
<tr>
<td></td>
<td><strong>Logs</strong></td>
</tr>
<tr>
<td>5</td>
<td>CA Server Log (login/logout/reboot)</td>
</tr>
<tr>
<td>6</td>
<td>RA Server Log (login/logout/reboot)</td>
</tr>
<tr>
<td>7</td>
<td>Repository Server Log (login/logout/reboot)</td>
</tr>
<tr>
<td>8</td>
<td>Access log of the CA server room</td>
</tr>
<tr>
<td></td>
<td><strong>CA server room</strong></td>
</tr>
<tr>
<td>9</td>
<td>Inspection of the CA server room and related devices</td>
</tr>
<tr>
<td></td>
<td><strong>Certificates</strong></td>
</tr>
<tr>
<td>10</td>
<td>Self signed certificate, fingerprint</td>
</tr>
<tr>
<td>11</td>
<td>End entity certificates (Globus Server/Client, Unicore Server/Client, LDAP server)</td>
</tr>
<tr>
<td>12</td>
<td>CRL</td>
</tr>
</tbody>
</table>
Schedule

- **Interview and log check**
  - Principle 1: 13:30 ~ 14:20
  - Principle 2: 14:20 ~ 15:10
  - Principle 3: 15:10 ~ 16:00

- **Inspection of CA server, etc.**
  - 16:15 ~ 17:00
Sample interviewed issues

**Principle 1**
- How does an end entity know that his certificate has been issued?
- How does an end entity know that his certificate has been revoked?

**Principle 2**
- Who operates the CA system? Who knows the pass phrase for CA private key?
- Who can access to the backup media of CA private key?
- Who has a key of a safe box?
- How do you confirm the uniqueness of subject name?
- How do you generate a CRL if you receive multiple revocation requests at the same time?
Sample interviewed issues (cont’d)

Principle 3

- Who revises the CP/CPS? and Who authorizes the revision of CP/CPS?
- In which case do you assign a new OID to the CP/CPS?
- How do you inform end entities that the CP/CPS has been revised?
- How do you control access to the CA room?
- What kind of information do you archive?

Others

- How does RA communicate with CA?
Sample inspected issues

- **Principle 2**
  - HSM
  - A safe box
  - Revocation function of the CA system
  - Backup media of archive
  - Issued certificates

- **Principle 3**
  - CA room
# Summary of auditing

<table>
<thead>
<tr>
<th>Principle</th>
<th>Number of criteria</th>
<th>By document check</th>
<th>By Interview</th>
<th>By Inspection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1</td>
<td>13</td>
<td>13</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Principle 2</td>
<td>14</td>
<td>14</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>Principle 3</td>
<td>7</td>
<td>7</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Others</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Summary of auditing (cont’d)

Most interviewed issues should be described in CP/CPS.

- Basically, CP/CPS is the only way for giving end entities the information about the CA.

Advised issues

- Some issues must be described in CP/CPS
  - Procedures for revising CP/CPS
    - who does? who authorizes? how to inform end entities.
  - Access control to the CA room, CA system
  - other small issues

- Not all issued CRLs were archived
  - violate minimum CA requirements
  - AIST GRID CA will archive all issued CRLs.

- CA room is not dedicate for CA operation
  - The room was shared by other system engineers for cluster management.
  - We have made the CA room to be dedicated to the CA operation.
Summary of audit (cont’d, last)

The focuses of auditors

- How the CA private key is kept secure
- Issuing certificates must not be done by a single person.
  - how to implement multi-person control
- Enough records/logs must be archived so that we can trace anything if illegal accident would happen.
  - Server logs (login/logout/reboot)
  - Access logs to the CA room
    - Date, name, purpose, etc.
- Describe CP/CPS as rich as possible

Purpose of auditing

- Not the audit itself but to improve CA operation!
New CP/CPS: 1.0 -> 1.1

**Major Changes**

- Added revision history table change logs.
- Assigned a new OID (1.2)
- Changed AIST GRID PMA members.
- Detailed descriptions
  - Specification administration in Sections 8.1, 8.2, and 8.3.
    - Who will authorize new CP/CPS? and how?
  - Physical access to the CA server in Section 5.1.2.
    - Who can access to the CA server?
    - How the CA server room is protected?
    - How to implement multi-person control
  - Protection and backup procedure of records archival in Sections 4.6.3 and 4.6.4.
    - What kind of information are archived?
    - How the archived data is protected and verified?
New CP/CPS: 1.0 -> 1.1 (cont’d)

- **Major Changes**
  - **Detailed descriptions**
    - Compliance Audit in Section 2.7
      - Frequency, topics, actions,
    - Security Audit Procedures in Section 4.5.
      - Types of event recorded, protection and backup of audit log
    - Records Archival in Section 4.6
      - Types of event recorded, protection of archive
  - **Changed Certificate Profile**
    - Added CRL Distribution Points in extension field.
    - Added Issuer Alternative Name in extension field.
  - **Specify version number of AIST GRID CA Certificate and CRL Profile in Sections 7.1 and 7.2.**
X509v3 extensions of user cert issued by AIST GRID CA

X509v3 extensions:
  x509 Basic Constraints:[critical]
    CA:FALSE
    PathLenConstraint:NULL
  x509 Key Usage:[critical]
    digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, (0xf0)
  x509 Authority Key Identifier:
  x509 Subject Key Identifier:
  x509 Certificate Policies:
    policyID = 1.3.6.1.4.1.18936.1.11.2.2.1
    qualifierID = pkix-id-qt CPSurl
    qualifier = https://www.apgrid.org/CA/AIST/Production/AIST-CP-CPS-1.1.pdf
  x509 CRL Distribution Points:
    [0] dist-point :
    [0] fullName :
    [6] https://www.apgrid.org/CA/AIST/Production/a317c467.r0
  x509 Issuer Alt Name:
    [1] gridca@m.aist.go.jp