Checklist for MICS-based CAs

38th EUGridPMA & IGTF All Hands meeting
September 21 2016
Geneva, Switzerland

Eisaku Sakane
sakane@nii.ac.jp
National Institute of Informatics
Japan

National Institute of Informatics

Background

- All IGTF-accredited CAs must make a report of self-audit
- HPCI CA is based on MICS authentication profile, however, currently there is no official auditing checklist for MICS-based CA
- HPCI CA needs a checklist for MICS-based CA
- In addition, HPCI needs a checklist for MICS IdM itself because HPCI IdM has not been audited so far though HPCI IdM formally is independent of HPCI CA

Self Audit of HPCI CA

- Organizations to be audited or assessed:
  - HPCI CA (NII)
  - HPCI Operations Office (RIST)
    - manage HPCI-ID and user information associated with the HPCI-ID.
  - IdP Operating Organizations (Supercomputing centers)
    - manage accounts for Shibboleth authentication.
    - primary centers: Shibboleth IdPs
    - check centers: desks for initial vetting of identity
  - HPCI system providers (Supercomputing centers)
    - GSI-based SSH servers that communicate with the CA to obtain a grid-mapfile created by the CA.

IdM organizations

National Institute of Informatics

Auditing Checklist for MICS

- Checklist for MICS-based CA
  - The auditing checklist in GFD-I.169 is built based upon “Classic” Authentication Profile.
  - There are common check items in Classic and MICS.
  - We made a checklist for MICS-based CA by extracting MICS-specific features from MICS AP and by adding them to GFD-I.169.
- Checklists for MICS IdM
  - Currently HPCI IdM assessing list is practically operational audit because it is based on not IdM profile but operation manuals.
  - Maybe not applicable to the other MICS-based CA than HPCI

MICS-specific items (1/10)

1.1.5 Certificate Revocation (of 1.1 Certificate Authority)

29. In the event the end-entity identity in the IdM is compromised, affected issued certificates should be revoked.

30. The IdM manager must not assert identity attributes if identity data changes without validation or the traceability to the person is lost.

- In self-auditing HPCI CA, we checked items as follows:
  - check whether the CP/CPS describe the contents of the item
  - check whether the requirement is actually satisfied

MICS-specific items (2/10)

1.1.7 End Entity Certificates and Keys

47. For any renewal or rekeying of the certificate by the MICS:
    - The registered owner must authenticate to the IdM and
    - The MICS must follow the same identity translation requirements described above.

52. The CP/CPS must address how the IdM maintains persistence and traceability for entities that are eligible for a MICS certificate, and how name uniqueness is guaranteed.

MICS-specific items (3/10)

1.1.9 Audits

60. In order to establish the trust of the IdM itself, it is recommended that the IdM system make its periodic audits and reviews available to the CA.

MICS-specific items (4/10)

1.2.1 Entity Identification (of 1.2 Registration Authority)

1. A MICS PKI CA should define the role of Registration Authority (RA)and how these RAs interact with the IdM system process.

2. The initial vetting of identity for any entity in the primary authentication system that is valid for certification should be based on a face-to-face meeting and should be confirmed via photo-identification and/or similar valid official documents.

5. In the case of host or service entities, the initial registration should ensure that the association between the registered owner and the FQDN is correct, and sufficient information should be recorded to contact the registered owner.

MICS-specific items (5/10)

1.2.1 Entity Identification

6. In the case where the initial identity vetting is a distributed operation, these rules shall apply for all registration authority (RA)points and all identity validations that result in primary identities that can be translated by the MICS.
   Any distributed RA must have formal authority to recognize and establish end-entity identity.

9. The primary identity management system may contain other entities that do not qualify based on the above mentioned conditions, but it must not be possible for such entities to obtain valid credentials from the MICS.

MICS-specific items (6/10)

1.2.1 Entity Identification

10. All identities used to create end-entity certificates must be based on a described primary identity management (IdM) system.

11. A MICS authority must identify the organizational or federated identity management service that will be used to provide the authenticated identity to the MICS.

12. The organization or federation must provide details of how the IdM system creates and validates identities for its users, and this information must be detailed in the CP/CPS of the MICS.

MICS-specific items (7/10)

1.2.1 Entity Identification

13. The identity management (IdM) system containing the identity information of the organization or federation must also meet the following conditions:
    i. Re-usable private information used to authenticate end-entities to the IdM system must only be sent encrypted over the network when authenticating to any system (including any non-certificate issuing systems) that are allowed to use the IdM for authentication.
    ii. The end-entities must be notified of any certificate issuance, using contact information previously registered in the IdM (for example by electronic mail).
    iii. From the information stored in the IdM it must be possible to determine if the requestor's identity has originally been validated using all initial vetting requirements described above.

MICS-specific items (8/10)

1.2.1 Entity Identification

14. A second authentication element not published and not normally used to authenticate to the IdM (i.e. a reasonable private identity verification element) may be used to authenticate the end-entity for any certificate issuance. The CP/CPS must describe how the `private element' maps to the IdM identity and how it increases identity assurance. Answers to `private element' questions are collected either at initial face to face registration or out-of-band with RA verification.

MICS-specific items (9/10)

1.2.1 Entity Identification

15. The IdM used by the CA should be an identity management system that is also used to protect access to other critical resources -- e.g., payroll systems; financial transaction support; access control for highly valued resources -- and should be regularly maintained.
    Alternately, equivalent security mechanisms must be provided and described in detail and presented to the PMA with acceptance subject to PMA agreement.

- This stipulates the LoA of the MICS IdM.
- The HPCI IdM is not used to protect access to other critical resources than HPCI resources, however the HPCI IdM is the same level of identity management system as “Classic” RA.

MICS-specific items (10/10)

1.2.1 Entity Identification

16. The IdM system(s) of the organization or federation must be well protected, and all communications between the IdMs and the certificate issuance setup must be well secured.

Summary and Future Plan

- An auditing checklist for MICS CA is made based on MICS profile and GFD-I.169.
- There is room for improvement in the auditing checklist (alpha status)
- We need to do the following:
  - based on new IGTF profile: Authentication Assurance Profiles, Technical Guidelines
  - clear evidence and method for each item and describe them
  - make a MICS IdM profile
- Thank you for your cooperation !

National Institute of Informatics