Revocation in MICS §4.4

May 11-13, 2009
Zürich, Switzerland

Current MICS

- **4.4 Revocation**
- If the MICS implements revocation, revocation requests can be made by certificate holders, IdM managers and the MICS CA. These requests must be properly authenticated. Others can request revocation if they can sufficiently prove compromise or exposure of the associated private key.
- The IdM manager must suspend or revoke authentication if member data changes or the traceability to the person is lost. Suspension or revocation must last until identity is updated and confirmed according to IdM policies.
- Individual holders of a MICS certificate must request revocation if the private key pertaining to the certificate is lost or has been compromised, or if the data in the certificate are no longer valid.

Language is ambiguous

4.4 Revocation

- If the MICS implements revocation, revocation requests can be made by certificate holders, IdM managers and the MICS CA. These requests must be properly authenticated. Others can request revocation if they can sufficiently prove compromise or exposure of the associated private key.
- The IdM manager must **suspend or revoke authentication** if member data changes or the traceability to the person is lost. Suspension or revocation must last until identity is updated and confirmed according to IdM policies.
- Individual holders of a MICS certificate must request revocation if the private key pertaining to the certificate is lost or has been compromised, or if the data in the certificate are no longer valid.

1st proposal for clarification

- The IdM manager must **suspend or revoke eligibility to obtain a certificate** if traceability to the person is lost, and must ensure any changes to member data pertinent to certificate issuance are promptly made available to the MICS CA on issuance of any new certificate to a member.

- *And a lot of discussion followed*

MICS proposal from Marg

- The accreditation process must address how the IdM maintains persistence, uniqueness and traceability of each individual person.
- Certificates implicitly expire if the IdM can no longer provide persistence, uniqueness, and traceability to the individual.
- Upon loss of traceability, the CA Manager must suspend or revoke the ability for that individual to get a MICS certificate and should revoke any already issued certificates unless they expire in less than 1Ms."

- *which may suggest that you must be able to address the persistence of all possible individuals that might request a cert for each and every individual. Also, the 'implicitly expire' now comes across as something that will magically happen.*

Updated proposal

- 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.
- Certificates may be left to expire implicitly if the status of the entity in the IdM changes, if and only if traceability information to the individual is retained.
- Upon loss of traceability, the CA Manager must suspend or revoke the ability for that individual to get a MICS certificate and should revoke any already issued certificates unless they expire in less than 1Ms.

- *But also this caused a lot of discussion in the TAGPMA*

1st proposal for clarification

- The IdM manager must **suspend or revoke eligibility to obtain a certificate** if traceability to the person is lost, and must ensure any changes to member data pertinent to certificate issuance are promptly made available to the MICS CA on issuance of any new certificate to a member.
- *or*
- The IdM manager must suspend or revoke authentication **to the IdM** if …

- *What were the issues with originally proposed clarification?*

New text?

4.4 Revocation

- If the MICS implements revocation, revocation requests can be made by certificate holders, IdM managers and the MICS CA. These requests must be properly authenticated. Others can request revocation if they can sufficiently prove compromise or exposure of the associated private key.
- The IdM manager must suspend or revoke authentication **to the IdM** if member data changes or the traceability to the person is lost. Suspension or revocation must last until identity is updated and confirmed according to IdM policies.
- Individual holders of a MICS certificate must request revocation if the private key pertaining to the certificate is lost or has been compromised, or if the data in the certificate are no longer valid.