Mapping InCommon Bronze and Silver Identity Assurance Profiles to TAGPMA SLCS Requirements

Jim Basney, NCSA
jbasney@ncsa.uiuc.edu
March 25, 2009

1. Overview

The TAGPMA SLCS Profile specifies minimum requirements for a Certification Authority (CA) that issues short-term certificates based on authentication to an existing identity service. A SLCS CA's CP/CPS must document how the policies and procedures of both the CA and the identity service meet the profile's requirements.

This document explores the possibility of InCommon Federation identity providers (IdPs) acting as identity services to SLCS CAs[1] by comparing InCommon standards to the SLCS Profile requirements.

Each InCommon IdP makes publicly available[2] a Participant Operational Practices statement that outlines its identity management policies and procedures. However, given that there are approximately 80 InCommon IdPs today, and the number is growing, it is infeasible for a SLCS CA wishing to serve the entire InCommon community to individually research the practices and procedures of each IdP to document in the SLCS CP/CPS and present to the TAGPMA.

Instead, the SLCS CA must rely on common standards across InCommon. These standards are defined by Identity Assurance Profiles. Two such profiles are now available: Bronze and Silver.

This document proceeds as follows. The next section maps requirements from the SLCS Profile to standards in the InCommon Bronze and Silver profiles. The following section compares assessment practices. The final section draws conclusions.

This document is a discussion draft. Please post comments to tagpma-general@tagpma.org or jbasney@ncsa.uiuc.edu.

2. Mapping

This section maps requirements from the SLCS Profile to the InCommon Bronze and Silver profiles. Quotes from the SLCS Profile (v2.1b)

[1] Note that other relationships between SLCS CAs and InCommon IdPs are not considered.
[2] While these statements may be publicly posted, they are not easy for non-members of InCommon to find. http://www.incommonfederation.org/policies.cfm states, "Participant POP statements must be publicly posted on a website. The URLs for participant POPs are available to all Administrators via the secure adminstrative interface." It is not clear if InCommon intends for these statements to be hidden from non-members.

(http://www.tagpma.org/authn_profiles/slcs) are blue and quotes from the InCommon Bronze and Silver Identity Assurance Profiles (v1.0) (http://www.incommonfederation.org/assurance) are green.

The following processes must be described to the accrediting regional policy management authority of the IGTF ("the PMA"), and must be compliant with this Profile:

1. The procedures and policies that govern the initial identity validation
   InCommon Silver requires a written policy or practice statement that describes the identity verification process (Sec 4.2.2.1).
   InCommon Silver requires one or more of three identity-proofing criteria (existing relationship, in person proofing, and remote proofing) (Sec 4.2.2.3).
   No identity proofing requirements are specified for InCommon Bronze.[3]
2. How the primary identity management systems are managed and secured
   Sec 4.2.8 Technical Environment describes operational requirements for InCommon Silver. No requirements are specified for InCommon Bronze.
3. How the primary identity management systems are connected to the SLCS CA
   Sec 4.2.7 describes how identity assertions are sent securely to the relying party for both Silver and Bronze.
4. How the primary identity is translated to the X.509 certificate
5. How the chain of trust is protected during the translation process
   (Sec 4.2.7.3) (Silver and Bronze) The identity assertion must be either digitally signed by the verifier or obtained directly from the trusted entity (e.g. the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure transmission channel (e.g., TLS or SSL) that cryptographically authenticates the verifier and protects the assertion.

Sufficient information must be recorded and archived such that the association of the entity and the subject DN can be confirmed at a later date.

(Sec 4.2.2.2) (Silver) The minimum record retention period for registration data is seven years and six months beyond the expiration or revocation (whichever is later)… At a minimum, credentials shall include identifying information that permits recovery of the records of the registration associated with the credentials and a personal name that is associated with the identity Subject. In every case, given the issuer and the identifying information in the credential, it must be possible to recover the registration records upon which the credentials are based.

[3] However, the InCommon Identity Assurance Assessment Framework (v1.0) states, "While no identity proofing requirements are specified [for Bronze], it is expected that IdP operators use reasonable care when issuing authentication credentials to confirm that a single individual applies for and receives a given credential and its shared secret or similar credential verifier. Campuses are expected to issue such credentials to individual students, faculty, and employees that would be sufficient to protect campus academic information and intellectual property resources that should be available only to the campus community."

Qualifying IdMs must suspend or revoke authorization to use the service if the traceability to the person is lost. Suspension or revocation must last until identity is updated and confirmed according to IdM policies.

(Sec 4.2.4.2) (Silver and Bronze) IdP operator shall maintain record of the status of credentials and not authenticate credentials that have been revoked.

(Sec 4.2.4.6) (Silver) The IdP operator shall revoke credentials and tokens within 72 hours after being notified that a credential is no longer valid or is compromised to ensure that a claimant using the credential cannot successfully be authenticated by the IdP.

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

(Sec 4.2.1.8) (Silver and Bronze) The IdP operator shall be audited by an independent internal or external auditor at least every 24 months to ensure the operation's practices are consistent with the institution's policies and procedures for services of this type.

The Site/Organization must provide details of how the site identity management system creates and validates identities for its users. This information must be detailed in the CP/CPS of the SLCS CA.   The CP/CPS must describe:

1. How the identity (DN) assigned in the certificate is unique within the namespace of the issuer.
   (Sec 4.2.3.1) (Silver and Bronze) Each identity Subject shall self-select or be given at registration time a token (e.g., credential UserID) that is unique across all such elements in use by the IdP operator. An identity Subject can have more than one token, but a given token can only map to one identity Subject.
2. How it attests to the validity of the identity.
   (Sec 4.2.2.1) (Silver) The identity proofing and registration process shall be performed according to a written policy or practice statement that specifies the particular steps taken to verify identities.
3. How the identity (DN) assigned in the certificate will never be re-issued to another end-entity during the entire lifetime of the CA.
   (Sec 4.2.4.1) (Silver and Bronze) At the time of credential issuance, the IdP operator shall assign a unique identifier to the Subject's IdMS record. This identifier may be included in identity assertions that require a specific identifier for this Subject. This identifier must be unique among all such identifiers previously issued by the IdP operator and never be reassigned to a different person.
4. How it provides DN accountability, showing how they can verify enough identity information to trace back to the physical person for at least one year from the date of certification, and in keeping with audit retention requirements. In the event that documented traceability is lost, the DN must never be reissued.
   See (Sec 4.2.2.2) above.

3. Assessment

In this section, we compare the assessment procedures of TAGPMA and InCommon for the profiles under discussion.

TAGPMA uses a peer-review process for assessing CAs. Quoting the TAGPMA Charter (v2.2), "The TAGPMA will review members that run authentication services based on an approved Authentication profile and certify the operator is professionally committed to running the service to our specifications. This may include a physical compliance audit." The TAGPMA membership, which performs the assessment, consists of operators of accredited CAs and "relying parties representing communities that depend on the trustworthiness of [TAGPMA] certificates."

In contrast, according to the InCommon Identity Assurance Assessment Framework (v1.0), InCommon IdPs must "arrange for an independent audit… InCommon neither initiates nor performs such assessments or audits. The Auditor must provide the report required by InCommon and should send it directly to InCommon… The Auditor may be either an external contractor or may be a member of an internal audit office within the IdP operator's parent organization. The Auditor doing the review must be objective and independent of the IdP's organization following guidelines established by professional audit organizations such as The Institute of Internal Auditors *Standards for the Professional Practice of Internal Auditing*."

Ideally, in the case of a SLCS CA for which an InCommon IdP acts as the identity service, TAGPMA could rely on InCommon's assessment of IdPs, so that TAGPMA need not perform its own assessment of IdP policies and procedures. This is possible to the extent that the InCommon profiles satisfy TAGPMA's requirements for identity services.

4. Conclusions

Section 2 demonstrates that the InCommon Silver profile addresses all of the TAGPMA SLCS requirements. The Silver profile defines common standards for identity vetting, system management and security, recordkeeping, revocation, audits, and name management that appear to meet or exceed TAGPMA standards.

The InCommon Bronze profile also addresses many of the TAGPMA SLCS requirements regarding revocation, audits, and name management. TAGPMA should discuss whether InCommon Bronze meets the remaining SLCS profile requirements:

- *Document procedures and policies for initial identity validation*. While InCommon Bronze does not specify these procedures, every InCommon IdP must document them in its Participant Operational Practices (POP) statement. Could a SLCS CA simply refer to these statements, as maintained by InCommon, to satisfy the documentation requirement?
- *Document how identity management systems are managed and secured.* Again, while InCommon Bronze does not specify management and security requirements for these systems, the administrative processes, responsible persons, and technologies in use are documented in each IdP's POP statement. Is this sufficient for TAGPMA?

- *Sufficient information must be recorded and archived such that the association of the entity and the subject DN can be confirmed at a later date.* Can the SLCS CA maintain records sufficient to satisfy this requirement, without applying recordkeeping requirements to the IdPs?
- *Describe how they can verify enough identity to trace back to the physical person for at least one year from the date of certification.* What verified attributes would the SLCS CA need from the IdPs to meet this requirement?

If TAGPMA deems InCommon Bronze to be insufficient for satisfying the SLCS profile requirements, what are the minimum additional requirements the TAGPMA would place on Bronze IdPs? SLCS CAs could take responsibility for verifying that these additional requirements are met before peering with Bronze IdPs.

Further discussion in TAGPMA is required to answer the above questions.