InCommon Assurance 1.1 review guide

InCommon has published version 1.1 of the Identity Assurance Assessment Framework and Identity Assurance Profiles documents. On this page we present our general approach, describe the major changes in these documents from the 1.0.x versions, and suggest sections that are especially important for review.

- Overall approach
- Identity Assurance Assessment Framework (IAAF) changes
- Identity Assurance Profiles (IAP) changes

Overall approach

The work of the Refinement team had these objectives:

1. Respond to feedback from early-adopter campuses regarding provisions that were unclear or onerous.
2. Remove elements that were not justified by US government or InCommon community requirements.
3. Harmonize conflicting and out-of-date terminology.
4. Continue to meet requirements of the US government ICAM program for Assurance Levels 1 and 2 (Bronze and Silver).
5. Clarify the purpose and audience of each document.
6. Clearly indicate normative requirements; remove or appropriately distinguish examples and advice; describe requirements in terms of what must be achieved, as opposed to how to achieve it.
7. Reduce the number of referenced external documents, especially those that appear normative.

Identity Assurance Assessment Framework (IAAF) changes

- **Section 1: Introduction**
  Former section 1.2 (General Approach) removed, material moved to other sections.
- **Section 2: Identity Management Functional Model**
  This is a new section. It is intended to clearly define key terms and concepts used in Assurance Profiles, in the context of identity management systems typically used by InCommon participants. This section replaces the Glossary (Appendix A) in version 1.0.x. Identity management staff should review this section for consistency with their deployments.
- **Section 3: Identity Assurance Profiles** (previously Section 2)
  This section has been simplified to provide general information on the types of issues addressed in IAPs, rather than listing specific issues, and to remove apparent embedded requirements.
- **Section 4: Assessment and Audit of Identity Providers** (previously Section 3)
  This section has been modified to clarify the assessment and certification processes, as well as the roles of Audit and IT within those processes. Careful review of the proposed processes and responsibilities by auditors and CISOs is appreciated.
- **Appendix A: Glossary**
  Removed.

Identity Assurance Profiles (IAP) changes

- **Section 3: Silver and Bronze Profiles**
  New section, with material moved from Section 2 to clarify the intent of these profiles.
- **Section 4: Criteria**
  Criteria were removed if there was no justification for their presence based on US government or InCommon community requirements. Criteria were modified to be consistent with the terminology used in the IdM Functional Model (section 2 of the IAAF). "Suggested Evidence of Compliance" elements were removed.

- **4.2.1 Business, Policy and Operational Criteria**
  All previous criteria from this section have been removed, leaving only a requirement to be an InCommon Participant in good standing. Many of the removed criteria were called out as burdensome by early adopters.
- **4.2.2 Registration and Identity Proofing**
  It is no longer required to record identity proofing document numbers, only their type and issuer, and the requirement for 7.5-year retention of identity proofing records has been removed, making it subject to the Identity Provider Organization's applicable policy and law. The use of "existing relationship" in identity proofing was clarified.
- **4.2.3 Credential Technology**
  The criteria for "Subject modifiable shared secret" have been removed; they are no longer required by US government specs.
  The protection of authentication secrets has been clarified, particularly with respect to the scope of the situations where those secrets must be protected.
- **4.2.4 Credential Issuance and Management**
  Criteria for credential renewal/re-issuance were clarified. Criteria for record retention of credential issuance were added.
  The following criteria were removed. They were either duplicative of other criteria or were not justified by US government or InCommon community requirements.
  - Unique Subject identifier
  - Credential status
  - Credential status verification
  - Suspected credential compromise

- **4.2.5 Authentication Process**
  This section was rewritten to describe what must be achieved, as opposed to how to achieve it. Some material was moved to section 4.2.4.
- **4.2.6 Identity Information Management**
  Added criteria for IdMS's that store Subject records that all do not meet the same set of IAP criteria. Removed criteria for confirming attribute status.
- **4.2.7 Assertion Content**
  No significant changes.

- **4.2.8 Technical Environment**
  All criteria were modified to describe what must be achieved, as opposed to how to achieve it. Physical access log and Continuity of Operations Plan requirements were removed.