InCommon Assurance 1.2 Review Guide

InCommon has published candidate versions 1.2 of the Identity Assurance Assessment Framework and Identity Assurance Profiles documents as well as an example of the new Representation of Conformance document. On this page we present our general approach, describe the major changes in these documents from the 1.1 versions, and suggest sections that are especially important for review.

Overall approach

The revision team had these objectives:

1. Simplify the Bronze profile (equivalent to NIST LoA 1) to address the US government FICAM program's interest in promoting Bronze certification as a baseline for IdPs to authenticate to US government web sites.
2. Respond to feedback from early-adopter campuses regarding confusing audit requirements and provide further guidance on what's required for certification.
3. Update the documents to include missing items that were identified in developing the Assurance Legal Addendum.

Identity Assurance Assessment Framework (IAAF) changes

- **Section 1: Introduction**
  Reorganized section and added information about conformance to new versions of the IAAF and IAP.
- **Section 4: Assessment and Audit of Identity Providers**
  Provided for flexibility of audit requirements and referred to the IAP for specific information about each Profile.
- **4.2: Audit Process and Report**
  (Previously section 4.2 Audit Reports and 4.2.1 Conveyance to InCommon) Removed material that was not germane to the application process. Added a reference to the AICPA Statements on Standards for Attestation Engagements as an example of the audit framework auditors should be using. Cited an example report for further guidance. Clarified what the audit report should include. Clarified that the IdP Operator is responsible for submitting the summary report, along with a document outlining alternative means (if any were used).

Identity Assurance Profiles (IAP) changes

- **Section 3: Silver and Bronze Profiles**
  Clarified use of IAQs.
- **Section 4: Criteria**
  Modified and added criteria to reduce the burden of implementing Bronze.
- **4.2.1.4 (S) (B) IDPO Risk Management**
  Added periodic review of IdPO's IT operations to align with risk management objectives. For the Bronze profile, this requirement replaces the need for a formal IdMS audit, which had been a major barrier. This provision is not expected to be a burden for Silver certification.
- **4.2.3.2 (B) Basic Resistance to Guessing Authentication Secret**
  Clarified language.
- **4.2.3.4 (S) Stored Authentication Secrets**
  Removed cross reference.
- **4.2.3.5 (New - Bronze Only) Protection of Authentication Secrets**
  Added to reduce the burden of implementing password-protection requirements for Bronze-only applicants.
- **4.2.3.6 (S) Strong Protection of Authenticaton Secrets**
  Updated title to distinguish Silver from Bronze requirements.
- **4.2.5.6 Mitigate Risk of Credential Compromise**
  Removed the specific guidance on how to mitigate risk to align with the document approach taken in the 1.1 version.
- **4.2.7.2 (S) (B) Identity Assertion Qualifier (IAQ)**
  Added clarifying sentence that InCommon certifies IdPs as eligble to assert one more more qualifiers. And the IdPO must be capable of including the InCommon IAQ when the criteria are met for a subject.
- **Section 5 Determination of Conformance**
  This new section distinguishes how conformance with the Bronze and Silver profiles is requested by the IdPOs and how the new Representation of Conformance document supports Bronze as an option in lieu of the current audit.

Representation of Conformance (Example)

This document serves as an example of the final agreement that IdPOs would need to sign, in addition to the Assurance Addendum, to attest to conformance to the Bronze profile in lieu of a formal audit.