

Your logo here

**[Your University] InCommon Silver Profile version 1.2  
Assessment Report  
For Internal Use Only**

Table of Contents

Summary 3

Assessment Objective 3

Scope and Methodology 3

4.2.1 Business, Policy and Operational Criteria 4

4.2.2 Registration and Identity Proofing 7

4.2.3 Credential Technology 16

4.2.4 Credential Issuance and Management 20

4.2.5 Authentication Process 25

4.2.6 Identity Information Management 31

4.2.7 Assertion Content 32

4.2.8 Technical Environment 35

# Summary

*Your school* wishes to assert adherence to the InCommon Silver Identity Assurance Profile version 1.2.

# Assessment Objective

# Scope and Methodology

# 4.2.1 Business, Policy and Operational Criteria

(Note: To assist in comparison planning, the authors have included the relevant Profile abbreviations for each Silver criterion. **(B)** indicates that the numbered section applies to the Bronze IAP; **(S)** indicates that the numbered section applies to the Silver IAP.)

IdP Operators must have the organizational structures and processes to come into and remain in compliance with the provisions of this IAP.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.1 Business, Policy and Operational Criteria** | | |
| **Criteria** | **4.2.1.1 (S) (B) InCommon Participant**:  The IdPO must be an InCommon Participant in good standing in order to be considered for certification under this IAP. In this context, “good standing” means not in arrears with respect to financial obligations to InCommon nor out of compliance with other contractual obligations to InCommon. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.1 Business, Policy and Operational Criteria** | | |
| **Criteria** | **4.2.1.2**  **(S)(B)** **Notification to InCommon**: The IdP Operator must notify InCommon of any circumstance that may affect the status of its compliance with this IAP.  1. The IdP Operator must notify InCommon of any significant changes to its operation  that may affect the status of its compliance and hence its qualification under this IAP. Notification should occur no less than 30 days before the changes are to be made effective, or as soon as practicable after an unanticipated change is noted.  2. The IdPO must report to InCommon any breach of security or integrity of its IdMS  Operations that may affect the status of its compliance and hence its qualification under this IAP. A report must be made as soon as practicable after any such incident is noted. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.1 Business, Policy and Operational Criteria** | | |
| **Criteria** | **4.2.1.3**  **(S)(B)** **Continuing Compliance:** After initial certification by InCommon, IdP Operators must declare to InCommon continued compliance with profiles under this IAP at least every 3 years. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.1 Business, Policy and Operational Criteria** | | |
| **Criteria** | **4.2.1.4**  **(S)(B)** **IDPO Risk Management:** The IdPO's Information Technology operations must align with the organization’s risk management objectives as demonstrated by a periodic review process or other equivalent control. | | |
| **Management Assertion/Statements** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

# 4.2.2 Registration and Identity Proofing

Identity Proofing in this IAP uses verified government-issued ID or public records. Verified information is used to create a record for the Subject in the IdPO’s IdMS.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.2 Registration and Identity Proofing** | | |
| **Criteria** | **4.2.2.1 (S) RA Authentication:** Each RA must authenticate to the IdMS using a credential that meets or exceeds Silver requirements.  Communications between an RA and the IdMS shall be encrypted using an Approved Algorithm that also authenticates the IdMS platform. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.2 Registration and Identity Proofing** | | |
| **Criteria** | **4.2.2.2 (S) Identity Verification Process**  1. The identity proofing and registration process shall be performed according to written policy or practice statements that specify the particular steps taken by IdPO staff or systems to verify identities.  2. The above statement(s) shall address the primary objectives of registration and identity proofing, including:  • Ensuring a person with the claimed identity information does exist, and that the  identity information is sufficient to uniquely identify a single person within the  IdPO’s range of foreseeable potential Subjects;  • Ensuring that the physical person requesting registration is entitled to the claimed identity. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.2 Registration and Identity Proofing** | | |
| **Criteria** | **4.2.2.3 (S) Registration Records**  1. A record of the facts of registration shall be maintained by the IdPO.  2. The record of the facts of registration, shall include:  • Identity proofing document types and issuers;  • Full name as shown on the documents;  • Date of birth;  • Current address of record.  3. Records also must include revocation or termination of registration.  4. Registration records must be retained for 7.5 years beyond the expiration of any credential issued to the Subject by the IdPO. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

## 4.2.2.4 Identity Proofing

Prior to this process, the Subject supplies his or her full name, date of birth, and an address of record to be used for communication with the Subject, and may, subject to the policy of the IdPO, also supply other identifying information. For each Subject, the full name, date of birth and address of record must be verified using one or more of the following methods:

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.2 Registration and Identity Proofing**  **4.2.2.4 (S) Identity Proofing** | | |
| **Criteria** | **4.2.2.4.1 (S) Existing Relationship**  If the IdPO is a function of an enterprise, the identity proofing process may be able to leverage a pre-existing relationship, e.g., the Subject is an employee or student. Where some or all of the identity proofing done at the time the existing relationship was established is comparable to that required in §4.2.2.4.2 or §4.2.2.4.3 below, those results may be relied upon for this purpose. The IdPO’s Registration Authority (RA) shall confirm that the Subject is a person with a current relationship to the organization, record the nature of that relationship and verify that the relationship is in good standing with the organization. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.2 Registration and Identity Proofing**  **4.2.2.4 Identity Proofing** | | |
| **Criteria** | **4.2.2.4.2 (S) In-Person Proofing**  1. The RA shall establish the Subject’s IdMS registration identity based on possession of a valid current government photo ID that contains the Subject’s picture (e.g., driver’s license or passport), and either an address or nationality.  2. The RA inspects the photo ID and compares the image to the physical Subject.  The RA records the document type and issuer, the address given on the ID if  there is one, and the date of birth shown on the ID if there is one. If the ID  appears valid, the photo matches the physical Subject, and the ID confirms the  Subject’s date of birth, the RA authorizes issuance of Credentials.  3. If the address given on the ID does not confirm the Address of Record, the Address of Record must be confirmed as described in §4.2.2.5 below. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.2 Registration and Identity Proofing**  **4.2.2.4 Identity Proofing** | | |
| **Criteria** | **4.2.2.4.3 (S) Remote Proofing**  1. The RA shall establish the Subject’s IdMS registration identity based on possession of at least one valid government ID number (e.g., a driver’s license or passport) and either a second government ID number or financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number.  2. The RA verifies other information provided by the Subject using both of the ID numbers above through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, date of birth, and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. If this appears to be the case, the RA authorizes issuance of Credentials.  3. If the record checks do not confirm the Address of Record, it must be confirmed  as described in §4.2.2.5 below. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.2 Registration and Identity Proofing** | | |
| **Criteria** | **4.2.2.5 (S) Address of Record Confirmation**  The Address of Record must be confirmed before the Subject’s record can be considered to meet the requirements of this IAP. If the Address of Record was not confirmed as part of Identity proofing, then it must be accomplished by one of the following methods:  1. The RA contacts the Subject at the Address of Record and receives a reply from the  Subject; or  2. The RA issues Credentials in a manner that confirms the Address of Record supplied  by the Subject.  a. For a physical Address of Record, the RA requires the Subject to enter online  a temporary Secret from a notice mailed to the Subject’s Address of Record.  b. For an electronic Address of Record, the RA confirms the ability of the Subject  to receive telephone communications at a telephone number or e-mail at an  e-mail address.  Any Secret not sent over a Protected Channel shall be invalidated upon first use. | | |
| **Managemet Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.2 Registration and Identity Proofing** | | |
| **Criteria** | **4.2.2.6 (S) (B) Protection of Personally Identifiable Information**  Any personally identifiable information collected during registration or identity proofing must be protected from unauthorized disclosure or modification. | | |
| **Managemet Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

# 4.2.3 Credential Technology

These InCommon IAPs are based on use of “shared Authentication Secret” forms of identity Credentials. If other Credentials are used to authenticate the Subject to the IdP, they must meet or exceed the effect of these requirements.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.3 Credential Technology** | | |
| **Criteria** | **4.2.3.1 (S)(B)** **Credential Unique Identifier**    1. Each Credential issued by the IdPO shall include a unique identifier (e.g., userID, Distinguished Name, serial number) that distinguishes it from all other Credentials in use by the IdPO.  2. A Subject can have more than one Credential unique identifier, but a given Credential unique identifier must map to at most one Subject.  3. The IdPO shall clearly associate the Credential unique identifier to the Subject’s registration record in the IdMS, for use by the Verifier or other parties. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

**(4.2.3.2 Resistance to Guessing Authentication Secret has been omitted because it appears only in the Bronze Profile.)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.3 Credential Technology** | | |
| **Criteria** | **4.2.3.3 (S) Strong** **Resistance to Guessing Authentication Secret**  1. The Authentication Secret and the controls used to limit online guessing attacks shall ensure that an attack targeted against a given Subject’s Authentication Secret shall have a probability of success of less than 2-14 (1 chance in 16,384) over the life of the Authentication Secret. This requires that an Authentication Secret be of sufficient complexity and that the number of invalid attempts to enter an Authentication Secret for a Subject be limited.  2. The Authentication Secret shall have at least 10 bits of min-entropy to protect against an untargeted attack.  Refer to NIST Special Publication 800-63-1 [SP 800-63], Appendix A, for a discussion of Authentication Secret complexity and resistance to online guessing and how to calculate min-entropy | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.3 Credential Technology** | | |
| **Criteria** | **4.2.3.4**  **(S)** **Stored Authentication Secrets**: Authentication Secrets shall not be stored as plaintext. Access to encrypted stored Secrets and to decrypted copies shall be protected by discretionary access controls that limit access to administrators and applications that require access (see also §4.2.5.6).  Three alternative methods may be used to protect the stored Secret:  1. Authentication Secrets may be concatenated to a variable salt (variable across a group of Authentication Secrets that are stored together) and then hashed with an Approved Algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen Authentication Secret file are not useful to attack other similar Authentication Secret files. The hashed Authentication Secrets are then stored in the Authentication Secret file. The variable salt may be composed using a global salt (common to a group of Authentication Secrets) and the userID (unique per Authentication Secret) or some other technique to ensure uniqueness of the salt within the group of Authentication Secrets; or  2. Store Secrets in encrypted form using Approved Algorithms and decrypt the needed Secret only when immediately required for authentication; or  3. Any method protecting stored Secrets at NIST [SP 800-63] Level 3 or 4 may be used. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

**(4.2.3.5 Basic Protection of Authentication Secret has been omitted because it appears only in the Bronze Profile.)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.3 Credential Technology** | | |
| **Criteria** | **4.2.3.6**  (**S)** **Strong Protection of Authentication Secrets**  1. Any Credential Store containing Authentication Secrets used by the IdP (or the IdP’s Verifier) is subject to the operational constraints in §4.2.3.4 and §4.2.8 (that is, the same constraints as IdMS Operations). When Authentication Secrets are sent from one Credential Store to another Credential Store (for example in an account provisioning operation) Protected Channels must be used.  2. Whenever Authentication Secrets used by the IdP (or the IdP’s Verifier) are sent between services for verification purposes (for example, an IdP to a Verifier, or some non-IdP application to a Verifier), Protected Channels should be used, but Protected Channels without client authentication may be used.  3. If Authentication Secrets used by the IdP (or the IdP’s Verifier) are exposed in a transient fashion to non-IdP applications (for example, when users sign on to those applications using these Credentials), the IdPO must have appropriate policies and procedures in place to minimize risk from this exposure. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

# 4.2.4 Credential Issuance and Management

The authentication Credential must be bound to the physical Subject and to the IdMS record pertaining to that Subject as described in this section.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.4 Credential Issuance and Management** | | |
| **Criteria** | **4.2.4.1**  **(S)(B)** **Credential Issuance**  To ensure that the same Subject acts throughout the registration and Credential issuance process, the Subject shall identify himself or herself in any new transaction (beyond the first transaction or encounter) with information known only to the Subject, for example a temporary Secret which was established during a prior transaction or encounter, or sent to the Subject’s Address of Record. When identifying himself or herself in person, the Subject shall do so either by using a Secret as described above, or through the use of an equivalent process that was established during a prior encounter. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.4 Credential Issuance and Management** | | |
| **Criteria** | **4.2.4.2**  **(S)(B)** **Credential Revocation or Expiration**  1**.** The IdPO shall revoke Credentials and Tokens within 72 hours after being notified that a Credential is no longer valid or is compromised.  2. If the IdPO issues Credentials that expire automatically within 72 hours or less then the IdPO is not required to provide an explicit mechanism to revoke the Credentials. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.4 Credential Issuance and Management** | | |
| **Criteria** | **4.2.4.3**  **(S)(B)** **Credential Renewal or Re-Issuance**: A Subject must be authenticated for purpose of Credential renewal or re-issuance by any of the following methods:   1. By use of a non-expired and valid Credential. 2. By use of a single-use secret delivered to the Subject from the IdPO by means of a pre-registered out of band delivery mechanism. 3. The Subject may supply correct answers to pre-registered personalized questions designed to be difficult for any other person to know.   After expiration of the current Credential, if none of these methods is successful then the Subject must re-establish her or his identity with the IdPO per Section 4.2.2 before the Credential may be renewed or re-issued.  Authentication Secrets shall not be recovered; new Authentication Secrets shall be issued. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.4 Credential Issuance and Management** | | |
| **Criteria** | **4.2.4.4**  **(S)** **Credential Issuance Records Retention**: The IdPO shall maintain a record of the unique identifier and time of issuance or revocation of each Credential issued or revoked for a minimum of 7.5 years beyond the expiration of the Credential. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.4 Credential Issuance and Management** | | |
| **Criteria** | **4.2.4.5**  **(S)(B)** **Resist Token Issuance Tampering Threat:** The process or processes used by the IdPO in 4.2.4.1, 4.2.4.2, and 4.2.4.3 must enable the Subject to verify that the IdPO is the source of any token or Credential data they receive. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

# 4.2.5 Authentication Process

The Subject interacts with the IdP to prove that he or she is the holder of a Credential, enabling the subsequent issuance of Assertions.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.5 Authentication Process** | | |
| **Criteria** | **4.2.5.1**  **(S)(B)** **Resist Replay Attack**  The authentication process must ensure that it is impractical to achieve successful authentication by recording and replaying a previous authentication message. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.5 Credential Issuance and Management** | | |
| **Criteria** | **4.2.5.2**  **(S)(B)** **Resist Eavesdropper Attack**  The authentication protocol must resist an eavesdropper attack. Any eavesdropper who records all the messages passing between a Subject and a Verifier or relying party must find that it is impractical to learn the Authentication Secret or to otherwise obtain information that would allow the eavesdropper to impersonate the Subject. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.5 Credential Issuance and Management** | | |
| **Criteria** | **4.2.5.3 (S)(B)**  **Secure Communication**  Communication between Subject and IdP must use a Protected Channel. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.5 Credential Issuance and Management** | | |
| **Criteria** | **4.2.5.4 (S)(B)** **Proof of Possession**  The authentication process shall prove the Subject has possession of the Authentication Secret or Token. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.5 Credential Issuance and Management** | | |
| **Criteria** | **4.2.5.5**  **(S)(B) Resist Hijacking Threat**  Session maintenance methods implemented by the IdP shall resist session hijacking. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.5 Credential Issuance and Management** | | |
| **Criteria** | **4.2.5.6**  **(S)(B)** **Mitigate Risk of Credential Compromise**  The IdPO must have policies, practices, or guidelines in place that prohibit Subjects from sharing their Credentials and mitigate risks of a Subject's Credential being acquired by someone else through other means. Subjects must be informed of these policies, practices or guidelines and educated about the importance of keeping their Credentials secure. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

# 4.2.6 Identity Information Management

Subject records in the IdPO’s IdMS must be managed appropriately so that Assertions issued by the IdPO’s IdP are valid.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.6 Identity Information Management** | | |
| **Criteria** | **4.2.6.1**  **(S)(B)** **Identity Record Qualification:**  If Subject records in an IdMS do not all meet the same set(s) of IAP criteria, then the IdP must have a reliable mechanism for determining which IAQ(s), if any, are associated with each record | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

# 4.2.7 Assertion Content

The IdPO must have processes in place to ensure that information about a Subject’s identity conveyed in an Assertion of identity to an SP is from an authoritative source.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.7 Assertion Content** | | |
| **Criteria** | **4.2.7.1 (S)(B)** **Identity Attributes**  The actual meaning of any attribute values identified as attributes recommended for use by InCommon Participants should be consistent with definitions in the InCommon Attribute Summary [InC-AtSum]. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.7 Assertion Content** | | |
| **Criteria** | **4.2.7.2**  **(S)(B)** **Identity Assertion Qualifier (IAQ)**  An IdPO may be certified by InCommon to be eligible to include one or more InCommon IAQs as part of Assertions. The IdP **must not** include an InCommon IAQ that it has not been certified by InCommon to assert and **must not** include an IAQ if that Assertion does not meet the criteria for that IAP. The IdP must be capable of including an InCommon IAQ when the necessary criteria are met for the Subject. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.7 Assertion Content** | | |
| **Criteria** | **4.2.7.3**  **(S)(B) Cryptographic Security**  Cryptographic operations are required between an IdP and any SP. Cryptographic operations shall use Approved Algorithms.  The Assertion must be either:   * Digitally signed by the IdP; or * Obtained by the SP directly from the trusted entity (e.g., the IdP or Attribute Service) using a Protected Channel. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

# 4.2.8 Technical Environment

IdMS Operations must be managed to resist various potential threats such as unauthorized intrusions and service disruptions that might result in false Assertions of Identity or other erroneous communications.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.8 Technical Environment** | | |
| **Criteria** | **4.2.8.1 (S) Software Maintenance**  IdMS Operations shall use up-to-date supported software. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.8 Technical Environment** | | |
| **Criteria** | **4.2.8.2**  **(S) Network Security**  1. Appropriate measures shall be used to protect the confidentiality and integrity of network communications supporting IdMS operations. Protected Channels should be used for communications between systems.  2. All personnel with login access to IdMS Operations infrastructure elements must use access Credentials at least as strong as the strongest Credential issued by the IdPO | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.8 Technical Environment** | | |
| **Criteria** | **4.2.8.3 (S)** **Physical Security**  IdMS Operations shall employ physical access control mechanisms to restrict access to sensitive areas, including areas such as leased space in remote data centers, to authorized personnel. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Author:** |  |
| **Functional Area** | **4.2.8 Technical Environment** | | |
| **Criteria** | **4.2.8.4**  **(S) Reliable Operations**  IdMS Operations shall employ techniques to minimize system failures and ensure that any failures are not likely to result in inaccurate Assertions being sent to SPs. | | |
| **Management Assertion/Statement:** |  | | |

**Evidence of Compliance**

|  |  |
| --- | --- |
| **Reviewer’s**  **Notes:** |  |
| **Testing**  **Performed:** |  |
| **Reviewer’s Conclusions:** |  |
| **Date of Review** |  |
| **Applicable Documentation/Workpaper** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Assessment Area** | 4.2.2 Business, Policy and Operational Factors |
| **Author Signature** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Assessment Area** | 4.2.1 Business, Policy and Operational Factors |
| **IDP Operator Signature** |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | mm/dd/yyyy | **Assessment Area** | 4.2.1 Business, Policy and Operational Factors |
| **Executive Management Signature** |  | | |