InCommon®

Identity Assurance Profiles
Bronze and Silver

11/04/2008
Version 1.0

Executive Summary

Identity Assurance Profiles, as described in the InCommon Identity Assurance Assessment Framework, define the specific requirements that Identity Providers must meet in order to be eligible to include InCommon Identity Assurance Qualifier(s) in identity assertions that they offer to Service Providers. The reader is assumed to be familiar with the InCommon Identity Assurance Assessment Framework.

This document defines criteria used to assess Identity Providers that wish to qualify for InCommon Silver or Bronze identity assurance designation. These profiles are intended to be at least compatible with the Federal NIST Special Publication 800-63 "Level 2" and "Level 1" identity assurance levels. The requirements are directly applicable to Identity Providers that use shared secret models for identity credentials but stronger credentials, as defined in [SP 800-63], could be used as well.

InCommon Bronze designation requires that an Identity Provider support at least basic userID/password credentials with reasonably hard to guess passwords. Identity assertions may include a unique identifier for each identity Subject that should be usable in access control lists but further identity information may be not well known. InCommon Silver designation requires credentials with very hard to guess passwords and better credential management, reasonably verified personal information about each Subject, unique Subject identifiers that are never reassigned, and secure business and operational processes.

An identity provider that qualifies under Silver automatically also qualifies under Bronze. Identity providers that meet or exceed either of these qualifications are identified as compliant in the InCommon Identity Provider metadata and may include the appropriate Identity Assertion Qualifier(s) in identity assertions they provide.

Table of Contents

1 INTRODUCTION 1
2 SCOPE 1
3 TERMINOLOGY 3
4 CRITERIA 4
4.1 SUMMARY OF ASSESSMENT FACTORS 4
4.2 DESCRIPTION OF ASSESSMENT FACTORS 6
4.2.1 Business, Policy and Operational Factors 6
4.2.2 Registration and Identity Proofing 8
4.2.3 Digital Electronic Credential Technology 11
4.2.4 Credential Issuance and Management 13
4.2.5 Security and Management of Authentication Events 16
4.2.6 Identity Information Management 19
4.2.7 Identity Assertion Content 20
4.2.8 Technical Environment 21
5 REFERENCES 23
6 DOCUMENT HISTORY 23

1 INTRODUCTION

This document is part of InCommon's defined identity assurance service. Please refer to the InCommon Identity Assurance Assessment Framework (IAAF) for an overview. Additional information can be found at http://www.incommonfederation.org

This Identity Assurance Profile (IAP) document contains criteria used to assess Identity Provider (IdP) operators that wish to qualify for InCommon Silver or Bronze identity assurance designation. An IdP operator is an organization that registers identity Subjects, issues and manages digital identity credentials, maintains an identity information database or directory, and provides certain identity information to Service Providers (SPs) on behalf of the identity Subject. This type of IdP is called "assertion-based" because an identity Subject authenticates to the IdP and then the IdP provides identity information regarding the Subject to one or more SPs in identity assertion messages. InCommon's certification that an IdP operator meets the requirements of an IAP gives the SP a basis for trusting the identity assertion.

IdP operators that wish to qualify for Silver or Bronze certification must undertake an initial assessment against the requirements in this IAP and then engage an independent qualified auditor to review and attest to that assessment. IdP operators qualified under this IAP must undergo a re-assessment and audit at least every 24 months to ensure the organization's policies, procedures and practices remain consistent with the IAP.

2 SCOPE

The scope of this assessment profile includes issues regarding the nature of the IdP operator's organization, the process for Subject registration with the IdP operator, the type of the digital credential they are given, the handling of identity information about the Subject, and the identity assertion given to SPs. This IAP covers only how identity credentials and associated identity information for Subjects that are natural persons are issued and managed. A full description of the role and scope of an IAP document is contained in the InCommon IAAF.

In any assertion-based system, the identity Subject must be given one or more digital credential(s) with which to authenticate to their IdP. A common form of credential is a "UserID" and a "shared secret" (e.g., password) to be used for local authentication of the Subject to the IdP. This IAP assumes that sufficiently robust passwords are adequate for the purposes of these identity assertions. Stronger forms of digital identity credentials such as Kerberos or PKI certificates should satisfy the credential requirements of these profiles as well.

A password is the secret that a claimant keeps confidential and enters on-line only to verify ownership of his or her digital identity credential. Passwords are typically character strings and may vary in robustness against guessing by an unauthorized party. Passwords also encompass Personal Identification Numbers (PINs), which are considered a special form of password consisting of only decimal digits. This IAP defines requirements for the nature and handling of passwords used for authentication to the IdP.

If stronger forms of digital credentials are used, e.g., Kerberos or PKI certificates, the password provisions of this IAP may not apply. For example, a PKI certificate on a hardware token must have a PIN to protect it but this IAP does not define the strength of that PIN nor any requirement for certificate revocation in case the device is lost or the PIN compromised. Therefore, in these cases the IdP operator and independent auditor must use professional judgment in determining whether the stronger credentials meet or exceed the requirements in section 4.2.3 *Digital Electronic Credential Technology*. Examples include:

- Password-based systems that employ specialized client software for the password authentication protocol and access management to the SP;
- Systems that use passwords in conjunction with hardware tokens or specialized software;
- Systems where PINs are used in conjunction with physical tokens or specialized software.

This IAP **may not** apply to:

- PKI or other token-based systems where the relying party (SP) expects to directly verify the Subject's possession of her or his credential; or
- Systems that require an independent SP to know the Subject's "shared secret" (see section 4.2.5.6); or
- Other types of IdP services such as authorization assertions.

InCommon Bronze criteria are a subset of InCommon Silver criteria. These two IAPs may have different requirements for the same criterion, for example password or token strength. In this case, meeting the Silver requirement will also satisfy the Bronze requirement but not *vice versa*. InCommon Federation metadata will designate Identity Provider (IdP) operators that are Federation Participants and that meet or exceed the requirements of the Bronze IAP as qualified to assert the Bronze Identity Assurance Qualifier (IAQ) as part of identity assertions. Identity Provider operators that meet the requirements of the Silver IAP will be designated as qualified to assert both Bronze and Silver IAQs, as appropriate, as part of identity assertions.

A given IdP operator may support a diverse community of Subjects and may have different identity management processes and services for subsets of that community. For example, a campus IdP operator might support a basic level of identity assurance for most students and staff and support enhanced identity assurance for faculty and for staff that perform in roles that require it. A campus IdP operator might support "guest accounts" for visitors for which there is no formal identity assurance and hence assertions for those Subjects would not conform even to the Bronze IAP. It is also possible for a given Subject to have more than one type of credential with which to authenticate to the campus's IdP and the particular credential used might affect the relevant IAQ. An InCommon IdP operator that is certified by InCommon to provide identity assertions under more than one IAP must be able to associate the appropriate IAQ(s), if any, with each identity assertion it makes based on how the assertion Subject's identity has been managed with respect to the criteria in each IAP.

3 TERMINOLOGY

This document relies on terminology defined in NIST Special Publication 800-63 "*Recommendations for Electronic Authentication*", and the Federal OMB "*Guidance for E-Authentication for Federal Agencies*" as well as terms defined by InCommon. See the References section of the IAAF for bibliographic details. The IAAF, Appendix A: Glossary, provides definitions of terms used in this document.

4 CRITERIA

The criteria outlined below are organized by assessment topic, and will be applied cumulatively as discussed in Section 2, Scope. These criteria apply to the organization's IDP and its relevant functional unit, not to a parent organization directly.

4.1 Summary of Assessment Factors

This table summarizes all of the assessment factors defined for Bronze and Silver IAPs. Cells that are shaded gray do not apply to the particular profile. Each factor is described and defined in the sections following.

Assessment Area	Factors	Bronze	Silver
4.2.1 Business, Policy and Operational Factors	.1 Established legal entity		
	.2 Designated authority for IdMS and IdP services		
	.3 General Disclosures to identity Subjects		
	.4 Documentation of policies and practices	n/a	
	.5 Appropriate staffing	n/a	
	.6 Outsourced components	n/a	
	.7 Helpdesk	n/a	
	.8 Audit of IdMS operations		
	.9 Risk Management plan	n/a	
	.10 Logging of operations events	n/a	
4.2.2 Registration and Identity Proofing	.1 Identity Verification Process disclosure	n/a	
	.2 Retention of registration records	n/a	
	.3 Identity proofing	n/a	
	.3.1 Existing relationship with the organization	n/a	
	.3.2 In-person proofing	n/a	
	.3.3 Remote proofing	n/a	
4.2.3 Digital Electronic Credential Technology	.1 Unique credential identifier		
	.2 Subject modifiable shared secret		
	.3 Resistance to guessing shared secret		n/a
	.4 Strong resistance to guessing shared secret	n/a	
4.2.4 Credential Issuance and Management	.1 Unique Subject identifier		
	.2 Credential status		
	.3 Confirmation of delivery	n/a	
	.4 Credential status verification	n/a	
	.5 Suspected or attempted credential compromise	n/a	
	.6 Credential revocation	n/a	
	.7 Credential renewal or re-issuance	n/a	

Assessment Area	Factors	Bronze	Silver
4.2.4.7 Security and Management of Authentication Events	.1 Secure channel		n/a
	.2 End-to-end secure communications	n/a	
	.3 Proof of possession		
	.4 Session authentication		
	.5 Stored secrets		
	.6 Protected secrets	n/a	
	.7 Mitigate risk of sharing credentials		
	.8 Threat protection 1		
	.9 Threat protection 2	n/a	
	.10 Authentication protocols 1		n/a
	.11 Authentication protocols 2	n/a	
4.2.6 Identity Information Management	.1 Identity status management	n/a	
4.2.7 Identity Assertion Content	.1 Identity attributes		
	.2 Identity Assertion Qualifier		
	.3 Cryptographic security		
4.2.8 Technical Environment	.1 Configuration Management	n/a	
	.2 Network Security	n/a	
	.3 Physical Security	n/a	
	.4 Continuity of Operations	n/a	

4.2 Description of Assessment Factors

The assessment criteria and suggested evidence of compliance are presented below for each of the factors in each assessment area. The suggested evidence is not an absolute requirement; assessors should create an assessment program appropriate to the IdP operator to be assessed. Assessors may use subjective judgment if the suggested evidence for a particular criterion is not readily available but other relevant evidence might be substituted. In such a case, the assessor should provide a brief justification for such a decision.

In the tables that follow, Ⓑ indicates the criterion applies to the Bronze IAP;
Ⓢ indicates the criterion applies to the Silver IAP.

4.2.1 Business, Policy and Operational Factors

These are factors that indicate the identity service provider's readiness to support and operate a reliable operational service.

4.2.1.1 Ⓢ Ⓑ Established legal entity and identity management services

1. The institution responsible for the IdP operator shall be a valid legal entity.
2. The operational identity management system (IdMS) and IdP service(s) will be assessed as they stand at the time of the Assessment. Planned but not yet implemented upgrades or modifications are not to be considered during the assessment.

Suggested Evidence of Compliance

1. Articles of incorporation, Organizational Charter, Affidavit, etc.
2. Site visit to the IdP operator management and operational facilities.

4.2.1.2 Ⓢ Ⓑ Designated authority for IdMS and IdP services

The IdP operator shall be designated by executive management of the responsible institution to perform this service as required by the institution's policies.

Suggested Evidence of Compliance

Institution's organization documentation and either relevant policy or delegation memo from executive office responsible for the IdP function.

4.2.1.3 Ⓢ Ⓑ General disclosures to Identity Subjects

The IdP operator shall make available to the intended Subject community the terms and conditions under which it issues accounts, as well as the privacy policy which governs the release of identity attribute information for its identity Subjects.

Suggested Evidence of Compliance

1. Terms, Conditions, and Privacy policies posted on Website or equivalent.
2. Documentation describing how IdP operator will do this.

4.2.1.4 Ⓢ Documentation of policies and practices

1. The IdP operator shall have all security related policies and procedures documented that are required to demonstrate compliance.
2. Undocumented practices will not be considered evidence.

Suggested Evidence of Compliance

Copies of or on-line links to policies

4.2.1.5 Ⓢ Appropriate staffing

1. The IdP operator shall have sufficient numbers and levels of staff to operate its services and supporting infrastructure according to its stated policies and procedures.
2. The staff who operate the IdP services shall have the appropriate skills and abilities for their roles.

Suggested Evidence of Compliance

Roles and responsibilities defined in job descriptions for each staff member.

4.2.1.6 Ⓢ Outsourced components

1. Components of an IdP's services may be provided by third parties but all such arrangements that might impact these assurance profiles must be covered by a written binding contract.
2. Any contract for outsourced components of the IdP services shall have clear, appropriate and monitored requirements, where the agreement stipulates critical policies and practices that bear upon the assurance profile of the IdP services.
3. Contractor responsibilities that are not stipulated in their agreements will not be considered reliable during the assessment.

Suggested Evidence of Compliance

The existence of supporting contracts and agreements.

4.2.1.7 Ⓢ Helpdesk

A helpdesk shall be available for identity Subjects to resolve issues related to their credentials during the IdP operator's regular business hours, minimally 8 hours per day, Monday through Friday.

Suggested Evidence of Compliance

The existence and proper staffing of a help desk function.

4.2.1.8 Ⓢ Ⓑ Institutional Audit of IdMS operations

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. At the time of the required assessment for conformance with these IAPs, the most recent institutional audit shall have been performed within the last 12 months.[1]

Suggested Evidence of Compliance

A copy of latest audit results and IdP response.

4.2.1.9 Ⓢ Risk Management plan

The IdP shall demonstrate a risk management methodology that adequately identifies and mitigates risks related to the IdP operations. These considerations should include at a minimum:

- background checks on staff in sensitive positions;

[1] This is a separate requirement from the audit for compliance with this IAP. The two audits may be combined.

- controls on access and changes to critical data;
- strong digital credentials for access to critical systems;
- separation of duties where appropriate.

Suggested Evidence of Compliance

Risk Assessment documentation

4.2.1.10 Ⓢ Logging of operations events

The IdP operator shall log date, time, nature and outcome of all significant events related to identity management (e.g., issuance, vetting, revocation, reactivation, successful and failed authentication events, etc.) and retain such logs securely for at least 6 months after the date of the last entry.

Suggested Evidence of Compliance

The existence of logs and a retention policy.

4.2.2 Registration and Identity Proofing

Identity proofing is the process by which an identity service provider associates a specific identity Subject with the correct record in the IdP operator's IdMS or creates a new record. If a new record is created it must be seeded with basic information for that Subject that will help re-establish the Subject's association with that record if required at some time in the future, e.g. the credential has expired or there is a gap in the Subject's association with the IdP operator.

4.2.2.1 Ⓢ Identity Verification Process (IVP) disclosure

1. 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.
2. The practice statement shall address primary objectives of registration and identity proofing, including:
   - Ensuring a person with the applicant's claimed attributes does exist, and those attributes are sufficient to uniquely identify a single person within the IdP operator's range of foreseeable potential Subjects;
   - Ensuring the applicant whose identity information is registered is in fact the physical person who is entitled to the claimed identity;
3. Personal identifying information collected as part of the registration process must be protected from unauthorized disclosure or modification.
4. The IdP operator shall publish its IVP and evidentiary requirements, to the extent necessary to indicate compliance with these IAP criteria. That is, the IdP operator is not *de facto* required to disclose all of its IVP processes and details. Rather, only enough information is required for the Assessment Team and Auditor to make an informed decision.

Suggested Evidence of Compliance

Documentation of procedures and requirements

4.2.2.2 Ⓢ Retention of registration records

1. A record of the facts of registration shall be maintained by the IdP operator or its representative (e.g., Registration Authority). This information should help re-establish the Subject's correct association with his or her IdMS entry if necessary at some future time.
2. The record of the facts of registration, shall, as a minimum, include:
   - Identity proofing document numbers;
   - Full name as shown on the documents;
   - Date of birth;
   - Current address of record (see IAAF glossary).
3. Records also must include revocation or termination of registration.
4. The minimum record retention period for registration data is seven years and six months beyond the expiration or revocation (whichever is later).
5. IdP operators also must conform with any corporate records retention policies, whatever laws apply to the corporate entity, and any state or Federal records retention requirements.
6. 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.

Suggested Evidence of Compliance

The records and logs obtained and kept

4.2.2.3 ⓢ Identity proofing

For each identity proofing mechanism employed by the IdP operator or its Registration Authority, one or more of the following three criteria must be met:

4.2.2.3.1 Existing Relationship

Employers and educational institutions which verify the identity of their employees, students or other affiliates by means comparable to those stated for In-person Proofing or Remote Proofing may be designated an RA by the IdP operator. The IdP operator shall confirm that the applicant 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. If the IdP operator's IdMS directory or database is separate from the institution's or RA's database, the IdP operator shall confirm that the applicant's name and address are consistent in both places.

Suggested Evidence of Compliance

The records of identity proofing.

4.2.2.3.2 In Person Proofing

1. The IdP operator's Registration Authority (RA) shall establish the applicant's IdMS registration identity based on possession of a valid current Government Picture ID that contains applicant's picture, and either an address or nationality (e.g., driver's license or passport)

2. RA inspects photo-ID, compares picture to applicant, records ID number, date of issuance and expiration, address if available, and date of birth. If ID appears valid and photo matches applicant then:
   a. If ID confirms the address of record,[2] authorize or issue credentials and send notice to the address of record; or
   b. If ID does not confirm the address of record,[3] issue credentials in a manner that confirms the address of record.

Suggested Evidence of Compliance

The existence of a standard documented process done by competent trained individuals.

4.2.2.3.3 Remote Proofing

1. The RA shall establish the applicant'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
   - a student or employee ID number; or
   - financial account number (e.g., checking account, savings account, loan or credit card); or
   - a utility service (e.g., electricity, gas, or water) account number.
2. RA verifies other information provided by applicant 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, address and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual.
3. Address confirmation and notification:
   a. RA sends notice to an address of record confirmed in the records check and receives a mailed or telephone reply from applicant; or
   b. RA issues credentials in a manner that confirms the address of record supplied by the applicant, for example by requiring applicant to enter on-line some information from a notice sent to the applicant; or
   c. RA issues credentials in a manner that confirms ability of the applicant to receive telephone communications at a telephone number or e-mail at an e-mail address associated with the applicant in existing records. Any secret sent over an unprotected channel shall be invalidated upon first use.

Suggested Evidence of Compliance

Documentation of the policy and process, and samples of records.

[2] See definition in section 4.2.2.2 above.

[3] Ibid.

4.2.3 Digital Electronic Credential Technology

These InCommon IAPs allow the use of "shared secret" forms of identity credentials; stronger credentials[4] may be used as well to authenticate the Subject to the IdP. The most common form of shared secret credentials is the traditional userID and password but other types exist as well. The basic model is that a Subject must enter a secret that only he or she knows and that can be used by the IdP's credential verification system to confirm that the subject of the credential is in fact offering the credential.

4.2.3.1 Ⓢ Ⓑ Unique credential identifier

1. 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.
2. An identity Subject can have more than one token, but a given token can only map to one identity Subject.

Suggested Evidence of Compliance

The documented mechanism in place to ensure uniqueness.

4.2.3.2 Ⓢ Ⓑ Subject modifiable shared secret

1. Each identity Subject shall self-select or be given a shared secret, e.g., PIN or password, that must be presented by a claimant asserting the credential. Such secret must meet the applicable requirements for resistance to guessing.
2. The identity Subject must be able to change his or her shared secret if the credential is still valid and the current secret has not been compromised. The new secret must meet the applicable requirements for resistance to guessing. If the Subject can not provide the current shared secret, the credential renewal procedure must be followed per section 4.2.4.7.

Suggested Evidence of Compliance

A documented process and mechanisms to accomplish this.

4.2.3.3 Ⓑ Resistance to guessing shared secret

The PIN (numeric-only) or password, and the controls used to limit on-line guessing attacks shall ensure that an attack targeted against a given identity Subject's PIN or password shall have a probability of success of less than 2^{-10} (1 chance in 1,024) success over the life of the PIN or password.

Refer to NIST [SP 800-63], Appendix A, and the NIST Shared Secret Entropy Spreadsheet to calculate resistance to online guessing.

Suggested Evidence of Compliance

1. Documented procedures and mechanisms that define a method of providing a mathematically adequate level of resistance.
2. Use of NIST Entropy Spreadsheet to show sufficient token strength.

4.2.3.4 Ⓢ Strong resistance to guessing shared secret

1. The PIN (numeric-only) or password, and the controls used to limit on-line guessing attacks shall ensure that an attack targeted against a selected user's PIN or password

[4] See NIST [SP 800-63]

shall have a probability of success of less than 2^{-14} (1 chance in 16,384) over the life of the PIN or Password.

2. The PIN (numeric-only) or password shall have at least 10 bits of min-entropy (a measure of the difficulty that an attacker faces to guess the most commonly chosen password used in a system) to protect against untargeted attack.

   Refer to NIST [SP 800-63], Appendix A, and the NIST Shared Secret Entropy Spreadsheet to calculate min-entropy and resistance to online guessing.

Suggested Evidence of Compliance

1. Documented procedures and mechanisms that define a method of providing a mathematically adequate level of resistance.
2. Use of NIST Entropy Spreadsheet to show sufficient token strength.

4.2.4 Credential Issuance and Management

How electronic identity credentials are issued and managed is critical to the assurance of identities that may be asserted by an IdP later. The credential represents the binding between the physical identity Subject and the IdMS database or directory record describing that entity.

4.2.4.1 Ⓢ Ⓑ Unique Subject identifier

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:

a. be unique among all such identifiers previously issued by the IdP operator;

b. never be reassigned to a different person.

This identifier need not be persistent, that is, the particular identifier for a given Subject could be changed if necessary.

Suggested Evidence of Compliance

The IdP operator's documentation of the procedures and mechanisms to achieve and ensure this uniqueness.

4.2.4.2 Ⓢ Ⓑ Credential status

IdP operator shall maintain record of the status of credentials and not authenticate credentials that have been revoked.

Suggested Evidence of Compliance

Documentation of mechanism in place to accomplish this

4.2.4.3 Ⓢ Credential Issuance Process

If the credential issuance process is a separate transaction from registration, these processes must be linked together to ensure that the credential is issued to the registered person. For simple passwords and where the credential is issued in person, this may be accomplished by observing the Subject make use of it. In the case of remote issuance, it may be accomplished by requiring the Subject to provide a secret phrase to the RA at the time s/he applies for a credential and then entering that phrase after entering his/her password for the first time. This also may be done by requiring subsequent entry of a temporary secret provided at registration time in person, or sent to the subject by way of:

a. Postal address of record such as that used for delivery of sensitive personal communications to that individual; or

b. Cell phone or telephone number of record.

Suggested Evidence of Compliance

Documentation of the credential issuance process.

4.2.4.4 Ⓢ Credential status verification

IdP operator shall provide a secure automated mechanism to allow the credential verifier to determine credential status during authentication of the claimant's identity. Acceptable mechanisms for credential status verification include, but are not limited to:

- Database lookup;
- Digitally signed revocation list;
- Status Responder.

In addition, IdP operator must ensure that credential status is available to verifier at least 99% of the time, inclusive of scheduled downtime,

Suggested Evidence of Compliance

Documentation of mechanism as implemented; system logs of down time for credential verifier.

4.2.4.5 Ⓢ Suspected or attempted credential compromise

1. If some type of compromise of a Subject's password is suspected, the IdP must not include the Silver IAQ as part of identity assertions for that Subject until the password has been reset successfully by the identity Subject.

   The identity Subject must be notified of this event as soon as possible.

   The IdP may include the InCommon Bronze IAQ during the period between suspected compromise and shared secret reset.

2. If a credential verifier detects 10 or more successive failed attempts to submit an authentication secret for a given credential within 10 minutes, this could indicate a brute force attack on the Subject's credential.[5] In this case the IdP must take at least one of the following steps:

   A. The IdP's credential verifier shall insert a 30 second delay before acting on password submission from that IP address until a verification is successful. If the failed attempts continue for more than 48 hours, the Subject shall be notified and required to reset her or his password; or

   B. The IdP shall not include the Silver IAQ as part of identity assertions for this Subject until the Subject resets her or his password (the Bronze IAQ still may be included); or

   C. Lock out use of this Subject's account until the Subject resets her or his password.

Suggested Evidence of Compliance

Documentation of processes and mechanisms to effect and demonstrate this.

4.2.4.6 Ⓢ Credential revocation

1. 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.
2. If the IdP operator issues credentials that expire automatically within 72 hours or less then the IdP operator is not required to provide an explicit mechanism to revoke the credentials.

Suggested Evidence of Compliance

Documentation of the mechanism in place to effect and demonstrate this.

[5] A slower rate of such an attack would take far too long to complete. See [SP 800-63], Appendix A, Section A.3

4.2.4.7 Ⓢ Credential renewal or re-issuance

Appropriate policy and process must be in place to ensure that any new credential and/or authentication secret, e.g., password, is provided only to the actual credential subject should it be necessary to renew an authentication secret, e.g., due to suspected compromise or the Subject having forgotten the secret, or to reissue a credential due to expiration. This process must be at least as trustworthy as the process used for initial issuance of the credential.

Proof-of-possession of an unexpired current authentication secret shall be demonstrated by the Claimant prior to the IdP allowing renewal or re-issuance. If the Claimant can not supply the current authentication secret, supplying answers to pre-registered personalized questions can suffice. If this "question and answer" method is used it must meet the requirements for shared secrets described in section 4.2.3 (strong resistance to guessing, etc).

Authentication secrets shall not be recovered; new secrets shall be issued. All interactions shall occur over a protected channel such as SSL/TLS.

After expiration of the current credential or authentication secret, renewal and re-issuance shall require the Subject be vetted again as described in section 4.2.2.

Suggested Evidence of Compliance

Documentation of the mechanism in place to effect and demonstrate this.

4.2.5 Security and Management of Authentication Events

An authentication event occurs when a Subject ("claimant") offers his or her credential to a credential verifier and proves the right to that identity binding. Such an event might occur at the time an identity assertion is needed or some amount of time before that point if the verifier supports a "single sign-on" stateful mechanism.

4.2.5.1 Ⓑ Secure Channel

Any secret used by a claimant during the authentication event supporting an identity assertion shall be encrypted if transmitted across any shared network that is not managed by the IdP operator or, if applicable, its parent organization.

Suggested Evidence of Compliance

Policy statement and mechanism to demonstrate this.

4.2.5.2 Ⓢ End-to-end secure communication

Under this IAP, cryptographic operations are required between claimant and verifier in order to ensure an end-to-end secure communications channel.

Suggested Evidence of Compliance

Documentation of procedures and mechanisms to properly encrypt the communications.

4.2.5.3 Ⓢ Ⓑ Proof of Possession

The authentication protocol shall prove the claimant has possession of the authentication password or token. For simple passwords, this should be accomplished by successful entry of the shared secret as determined by the verifier. For one-time passwords, the ability to enter a valid "next password" is sufficient. For PKI credentials, the ability of the Subject to prove possession of the private key would be sufficient. Other types of credentials may accomplish this in different ways.

Suggested Evidence of Compliance

Technical documentation and mechanism to demonstrate this.

4.2.5.4 Ⓢ Ⓑ Session Authentication

Session tokens shall be cryptographically authenticated. For example, session cookies must be encrypted, digitally signed, or contain a Hash-based Message Authentication Code. NIST approved cryptographic and or hash standards must be used.

Suggested Evidence of Compliance

Technical documentation and mechanism to demonstrate this.

4.2.5.5 Ⓢ Ⓑ Stored Secrets

Secrets such as passwords or PINs 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 shared secret:

1. Passwords may be concatenated to a salt and/or username and then hashed with an Approved Algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. The hashed passwords are then stored in the password file; or
2. Store shared secrets in encrypted form using Approved Encryption Algorithms and modes and decrypt the needed secret only when immediately required for authentication; or
3. Any method protecting shared secrets at NIST [SP 800-63] Level 3 or 4 may be used.

Suggested Evidence of Compliance

Documentation of the policy, procedure and mechanisms used to accomplish this, including documentation of implementation and testing.

4.2.5.6 Ⓢ Protected secrets

Any secret (e.g., password, PIN, key) involved in authentication shall not be disclosed to third parties by verifier or IdP, with the following exceptions:

- Sharing of session (temporary) shared secrets may be provided by the IdP to independent systems that must verify the secret;
- Long-term secrets and session (temporary) secrets can be shared with infrastructure elements controlled by the IdP operator or managed by an entity with which the IdP operator has a contract or other written agreement that defines adequate controls to mitigate risk of inappropriate disclosure of those secrets.

Suggested Evidence of Compliance

Documentation of mechanism in place to demonstrate and ensure this.

4.2.5.7 Ⓢ Ⓑ Mitigate risk of sharing credentials

Measures shall be taken to reduce the risk of an identity Subject intentionally compromising his/her token to repudiate authentication. These should include one or more of the following, as appropriate:

- Periodic confirmations that identity Subjects understand and will comply with security policy requirements;
- Confirmations of sensitive on-line transactions through a separate channel (such as electronic mail);
- Reminders to identity Subjects that sharing of credential tokens is prohibited.

Suggested Evidence of Compliance

Documentation including the policy, procedures and description of the mechanisms to accomplish this.

4.2.5.8 Ⓢ Ⓑ Threat protection 1

The authentication protocol must resist:

- On-line guessing – passwords or other authentication secrets must meet or exceed the required entropy and min-entropy criteria as determined using the NIST Password Entropy spreadsheet for the assurance profile being asserted.

- Replay – ensure that it is impractical to achieve successful authentication by recording and replaying a previous authentication message.

Suggested Evidence of Compliance

Documentation including the policy, procedures and description of the mechanisms to accomplish this.

4.2.5.9 Ⓢ Threat protection 2

The authentication protocol must resist an eavesdropper attack. Any eavesdropper who records all the messages passing between a claimant and a verifier or relying party must find that it is impractical (see IAAF Glossary) to learn the password or to otherwise obtain information that would allow the eavesdropper to impersonate the claimant.

Suggested Evidence of Compliance

Documentation including the policy, procedures and description of the mechanisms to accomplish this.

4.2.5.10 Ⓑ Authentication protocols 1

Authentication protocol types allowed under this IAP are:

- *Challenge-response password* – verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (often by hashing the challenge and secret together) to generate a response that is sent to the verifier.
- Any protocol allowed by the Silver IAP.

Suggested Evidence of Compliance

Documentation of the mechanism as implemented.

4.2.5.11 Ⓢ Authentication protocols 2

The authentication protocol types allowed under this IAP are:

- *Tunneled password* – claimant who provides a password does so through a secure (encrypted) TLS protocol session (tunneling).
- *Zero knowledge-base password* – claimant who provides password does not tell receiver anything about the password the receiver does not already know.

Suggested Evidence of Compliance

Documentation including the policy, procedures and description of the mechanisms to accomplish this.

Documentation of the operational IdP system.

4.2.6 Identity Information Management

Identity is the set of information correctly associated with an identity Subject. Identity assurance profiles attempt to reassure a Relying Party that identity information offered by an IdP can be trusted to a known degree. The Relying Party must decide for itself whether this reassurance is sufficient for its own purposes.

4.2.6.1 Ⓢ Identity status management

If the IdP operator is an independent service organization, identity attributes required by this IAP must be re-confirmed at a minimum frequency of every 2 years, or when notified by the identity Subject of a change.

If the IdP operator is part of a larger organization that is maintaining a continuing relationship with the identity Subject, identity attributes required by this IAP that are developed as part of that relationship and must be maintained reliably as part of the business processes for managing that continuing relationship with the Subject are assumed to be valid. Otherwise the requirement above for this factor applies.

Suggested Evidence of Compliance

Documentation of any reviews and audits to support the reliability of the identity attributes the IdP will offer to a Relying Party.

4.2.7 Identity Assertion Content

An identity assertion is the critical message that an IdP service sends to a Relying Party. It must be formed from reliable information and sent securely to the Relying Party. Some 'real time' information may be required in an assertion, e.g. details of the authentication event.

4.2.7.1 Ⓢ Ⓑ Identity Attributes

Identity attributes as used by InCommon are described on the InCommon Federation Attribute Overview web page. Specific attributes recommended for use by all IdPs and SPs are a described on the InCommon Federation Attribute Summary web page. The actual meaning of any attribute values identified as attributes recommended for use by InCommon Participants **must** be consistent with definitions in the most recent Attribute Summary document.

Suggested Evidence of Compliance

Documentation of the IdP operator's service and identity management descriptions.

4.2.7.2 Ⓢ Ⓑ Identity Assertion Qualifier (IAQ)

An IdP operator may be certified by InCommon to be able to include one or more InCommon IAQs as part of identity 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 identity assertion does not meet the criteria for that IAP.

Suggested Evidence of Compliance

IdP's documentation regarding how the IdP operator has been certified for each IAQ and how IAQs are assigned to assertions.

4.2.7.3 Ⓢ Ⓑ Cryptographic security

Cryptographic operations are required between an IdP's assertion provider and any Relying Party. Cryptographic operations shall be done in compliance with cryptographic techniques that are specified or recommended by NIST.

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.

Suggested Evidence of Compliance

Documentation of the system as implemented, or a statement from the software provider or developer regarding implemented cryptographic standards.

4.2.8 Technical Environment

The server and database platforms used by an IdP service must be configured to resist unauthorized intrusions and disruptions. Robust or redundant platforms help ensure continuity of service. Change management helps ensure that the state of all service platforms is known at any point in time.

4.2.8.1 Ⓢ Configuration Management

The IdP operator shall demonstrate a Configuration Management methodology that includes at least:

a. Version control for software system components;

b. Timely identification and installation of all applicable patches for any software used in managing or provisioning of the IdP service;

c. Logging of all software and configuration changes.

Suggested Evidence of Compliance

Documentation including CM logs and other documents.

4.2.8.2 Ⓢ Network security

1. The IdP operator shall protect their internal communications and systems with appropriate measures if such internal communications are transmitted across any shared network where the active components are not managed by the IdP operator or, if applicable, its parent organization. Such measures should mitigate against threats including eavesdropper, replay, verifier impersonation, DNS hijacking and man-in-the-middle attacks (See NIST [SP 800-63], section 8.1.1)
2. Appropriate network intrusion detection and prevention measures should be in place.

Suggested Evidence of Compliance

Documented protection measures for communications systems.

4.2.8.3 Ⓢ Physical security

The IdP operator shall employ physical access control mechanisms to ensure access to sensitive areas, including areas such as leased space in remote data centers, is restricted to authorized personnel. Access logs should document both entrance and exit of individuals.

Suggested Evidence of Compliance

Documentation of policy, procedures and mechanisms that provide physical access controls, including:

- Lock types and key distribution and retrieval
- Access lists and logs
- Procedures for guest or one-time entry

4.2.8.4 Ⓢ Continuity of Operations

1. The IdP operator shall employ mitigation techniques to ensure system failures do not result in false positive authentication errors.
2. The IdP operator should have a Continuity of Operations Plan (COOP) that covers disaster recovery and resilience of the IdP Subject authentication and identity

assertion service. Priority should be given to serving existing Subjects rather than registering new Subjects. If no COOP for this service exists, Subjects should be made aware of this fact.

NOTE: Service level agreements with Subjects are not assessment criteria for this factor; they are contractual arrangements between the parties.

Suggested Evidence of Compliance

1. Documentation of procedures and mechanisms that provide resistance to false positives
2. Documentation of Continuity of Operations / Disaster Recovery plan and the results from the last test of the plan or equivalent documents.

5 REFERENCES

For a Glossary and Acronym definitions, see the [IAAF].

[IAAF] InCommon "**Identity Assurance Assessment Framework**", version 1.0, September 2008

[eAuth CAP] Federal E-Authentication "**Password Credential Assessment Profile**", Release 2.0.0, March 16, 2005.

[SP 800-63] "**Electronic Authentication Guidelines**" NIST Special Publication 800-63-1

[Entropy spreadsheet] NIST "**PIN and Password Evaluation Spreadsheet**", version 2.0.0 http://www.cio.gov/eauthentication/documents/CommonCAP.xls

[InC-Attr-Ovr] "**InCommon Federation Attribute Overview**" http://www.incommonfederation.org/attributes.html

[InC-Attr-Sum] "**InCommon Federation Attribute Summary**" http://www.incommonfederation.org/attributesummary.html

[eduPerson] "**eduPerson Object Class**" http://www.educause.edu/eduPersonObjectClass/949

6 DOCUMENT HISTORY

This document was developed initially by the InCommon Federation Technical Advisory Committee. The overall concept was derived from the Federal e-Authentication "Password Credential Assessment Profile" Release 2.0.0 and NIST Special Publication 800-63-1.

Editors

David Wasley	Steven Carmody	RL "Bob" Morgan
John Krienke	Renee Shuey	Tom Barton
Karl Heins	Virginia Luke	David Walker

Status	Release	Date	Comments	Audience
Public	1.0	4 Nov 2008	First full release for implementation	Open