Identity Assurance Profiles
Bronze and Silver

November 30, 2012
Version 1.2
Rev.4
FICAM Draft

FICAM Updates 12/7/12 11:47 AM
Deleted: June 12

EXECUTIVE SUMMARY

Identity Assurance Profiles, as described in the InCommon Identity Assurance Assessment Framework, define the specific requirements that Identity Provider Operators 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 requirements for InCommon Silver and Bronze identity assurance certification. These profiles are intended to be compatible with the US federal government ICAM Trust Framework Provider Adoption Process, Levels of Assurance 1 and 2. The requirements are directly applicable to Identity Provider Operators that use Authentication Secret-based Credentials, but equivalent or stronger Credentials could be used instead.

InCommon Bronze certification requires that an Identity Provider Operator support at least basic authentication Credentials with moderately hard to guess Authentication Secrets. Assertions may include a unique identifier for each Subject registered in the Identity Provider Operator's Identity Management System that should be usable in access control lists, but further identity information need not be included or verified. InCommon Silver certification requires Credentials with hard to guess Authentication Secrets and better Credential management, reasonably well verified personal information about each Subject, unique Subject identifiers, and secure business and operational processes.

An Identity Provider Operator that is certified under the Silver profile also may wish to be certified to use the Bronze Identity Assurance Qualifier, for example, for Assertions that do not fully meet Silver requirements but do meet Bronze requirements. Identity Provider Operators that meet or exceed either of these qualifications are identified as certified in the InCommon Identity Provider metadata and may include the appropriate Identity Assertion Qualifier(s) in Assertions they provide.

TABLE OF CONTENTS

1 INTRODUCTION 1

2 SCOPE 1

3 SILVER AND BRONZE PROFILES 3

3.1 INCOMMON BRONZE IDENTITY ASSURANCE PROFILE 3

3.2 INCOMMON SILVER IDENTITY ASSURANCE PROFILE 3

4 CRITERIA 4

4.1 SUMMARY OF IDENTITY ASSURANCE CRITERIA 4

4.2 SPECIFICATION OF IDENTITY ASSURANCE REQUIREMENTS 7

4.2.1 Business, Policy and Operational Criteria 7

4.2.2 Registration and Identity Proofing 7

4.2.3 Credential Technology 9

4.2.4 Credential Issuance and Management 11

4.2.5 Authentication Process 12

4.2.6 Identity Information Management 13

4.2.7 Assertion Content 13

4.2.8 Technical Environment 13

5 DETERMINATION OF CONFORMANCE 14

5.1 CONFORMANCE WITH THE BRONZE PROFILE 14

5.2 CONFORMANCE WITH THE SILVER PROFILE 14

5.3 CONFORMANCE WITH BOTH THE SILVER AND BRONZE PROFILES 14

APPENDIX A: REFERENCES 1

APPENDIX B: ACRONYMS 1

APPENDIX C: DOCUMENT HISTORY 1

Deleted: 1
FICAM Updates 12/7/12 11:47 AM
Deleted: 1
FICAM Updates 12/7/12 11:47 AM
Deleted: 32
Ann West 12/7/12 12:01 PM
Deleted: 2
FICAM Updates 12/7/12 11:47 AM
Deleted: 32
Ann West 12/7/12 12:01 PM
Deleted: 2
FICAM Updates 12/7/12 11:47 AM
Deleted: 32
Ann West 12/7/12 12:01 PM
Deleted: 2
FICAM Updates 12/7/12 11:47 AM
Deleted: 43
Ann West 12/7/12 12:01 PM
Deleted: 3
FICAM Updates 12/7/12 11:47 AM
Deleted: 43
Ann West 12/7/12 12:01 PM
Deleted: 3
Unknown
Field Code Changed ... [1]
Ann West 12/7/12 12:01 PM
Deleted: 65
Ann West 12/7/12 12:01 PM
Deleted: 65
Unknown
Field Code Changed ... [2]
Unknown
Field Code Changed ... [3]
Ann West 12/7/12 12:01 PM
Deleted: 65
Unknown
Field Code Changed ... [4]
Ann West 12/7/12 12:01 PM
Deleted: 87
Unknown
Field Code Changed ... [5]
Ann West 12/7/12 12:01 PM
Deleted: 109
Unknown
Field Code Changed ... [6]
Ann West 12/7/12 12:01 PM
Deleted: 1110
Unknown
Field Code Changed ... [7]
Ann West 12/7/12 12:01 PM
Deleted: 1211
Unknown
Field Code Changed ... [8]
Ann West 12/7/12 12:01 PM
Deleted: 1211
Unknown
Field Code Changed ... [9]
Ann West 12/7/12 12:01 PM
Ann West 12/7/12 12:01 PM
Unknown
Field Code Changed ... [10]
Unknown
Field Code Changed ... [11]
Ann West 12/7/12 12:01 PM
Unknown
Field Code Changed ... [12]
Ann West 12/7/12 12:01 PM
Ann West 12/7/12 12:01 PM

1 INTRODUCTION

This document is part of InCommon's Identity Assurance Program. Please refer to the InCommon Identity Assurance Assessment Framework (IAAF) for an overview and for information on how InCommon certifies that an IdP Operator (IdPO) satisfies the requirements of this Identity Assurance Profile (IAP). Additional information can be found at http://www.incommon.org

Certain terms used in this document refer to elements of the InCommon identity management functional model as defined in the InCommon IAAF, Section 2. Such terms are capitalized in this document.

2 SCOPE

This IAP document contains requirements that IdPOs must satisfy if they wish to qualify for InCommon Silver or Bronze assurance designation. These requirements apply specifically to IdPOs that authenticate Subjects directly using credentials that the IdPO issues and then provide Assertions of Identity tailored to the needs of cooperating Service Providers (SPs). This IAP applies only for Subjects that are natural persons.[1]

The IAP includes issues regarding the process for Subject registration with the IdPO's IdMS, the digital Credentials they are given, the handling of identity information about the Subject, and the Assertion conveyed to SPs. It is not required that all Subject records in a given IdMS meet the criteria in this or any IAP. However, the IdP must be able to determine which Subject records do meet all relevant criteria and include only the appropriate assurance qualifier(s) in Assertions it issues.

An IdPO issues to a Subject one or more digital Credential(s) with which to authenticate to that IdPO's IdP. This IAP addresses primarily Credentials based on an Authentication Secret used for authentication of the Subject to the IdP. Equivalent or stronger[2] forms of digital Credentials such as one-time Authentication Secret devices, PKI certificates or other secure technologies could satisfy the Credential requirements of these profiles as well.

If other types of digital Credentials are used, the Authentication Secret requirements of this IAP may not apply. In such cases the IdPO and its independent auditor must use professional judgment in determining whether the other type of Credentials meet or exceed the requirements in §4.2.3. Examples include:

- Authentication Secret-based systems that employ specialized client software for the Authentication Secret authentication protocol and access management to the SP;
- Systems that use Authentication Secrets in conjunction with Tokens or specialized software;
- Systems where PINs are used in conjunction with Tokens or specialized software.

The IdPO is responsible for ensuring conformance with the requirements and criteria defined in this IAP regardless of how or where they are implemented, including outsourced

[1] See http://www.nolo.com/dictionary/natural-person-term.html
[2] See NIST [SP 800-63] for a discussion of Credential strength.

or delegated arrangements.

3 SILVER AND BRONZE PROFILES

This InCommon IAP document establishes requirements for IdPOs under two assurance profiles: Bronze, which represents a minimal formal set of requirements and Silver, which adds more stringent requirements. InCommon Bronze and Silver are intended to be compatible with US federal government Identity, Credential, and Access Management (ICAM) Trust Framework Provider Adoption Process (TFPAP) Levels of Assurance 1 and 2. They also include requirements regarding support for InCommon-recommended Identity Attributes.

InCommon Bronze requirements are fewer than InCommon Silver requirements. In some places these two IAPs have different requirements for the same criterion where the Bronze criterion is less stringent than that for Silver, for example, in the required Authentication Secret strength. Thus, an IdPO meeting the Silver requirement may be able to satisfy the Bronze requirement as well. InCommon Federation metadata will identify IdPs that are operated by InCommon-certified IdPOs and that meet or exceed the requirements of the Bronze IAP as qualified to assert the Bronze Identity Assurance Qualifier (IAQ) as part of Assertions and IdPs that meet the requirements of the Silver IAP as qualified to assert Silver IAQs, as appropriate, as part of Assertions. A given IdP may be certified to assert either or both IAQs but must ensure that only appropriate IAQs are associated with each Assertion.

3.1 INCOMMON BRONZE IDENTITY ASSURANCE PROFILE

The InCommon Bronze identity assurance profile focuses on sequential identity, that is, reasonable assurance that the same person is authenticating each time with a particular Credential. Assertions under this profile are likely to represent the same Subject each time a Subject identifier is provided.

While no identity proofing requirements are specified, it is expected that IdPOs use reasonable care when issuing Credentials to confirm that a single individual applies for and receives a given Credential and its Authentication Secret.

InCommon Bronze qualified Assertions are typically usable by individuals seeking access to online information resources licensed to an organization and for which the Subject is an eligible user. They also may be usable for access to online services where the SP will invoke other methods for linking of the Subject identifier to information the SP already has regarding individuals who should have access to its services.

3.2 INCOMMON SILVER IDENTITY ASSURANCE PROFILE

The InCommon Silver identity assurance profile builds on the Bronze profile requirements by adding criteria regarding individual Subject identity proofing and identity information records. Stronger Credential technology and Credential management are required as well.

The Silver IAP intends to assure a reasonably strong binding between the physical Subject and that Subject's digital Credential, and reasonably accurate information in Assertions. Credentials must at a minimum make use of Authentication Secrets that are sufficiently difficult to guess or intercept.

4 CRITERIA

The criteria outlined below are organized by functional area, as discussed in the IAAF, and will be applied cumulatively as discussed in Section 2 of this document. These criteria apply to the IdPO and are not dependent on any particular implementation architecture.

4.1 SUMMARY OF IDENTITY ASSURANCE CRITERIA

This table summarizes all of the identity assurance criteria defined for Bronze and Silver IAPs. Cells that are shaded and contain "n/a" do not apply to the indicated profile.

Functional Area	Criteria	Bronze	Silver
4.2.1 Business, Policy and Operational Criteria	1. InCommon Participant.	●	●
	2. Notification to InCommon	●	●
	3. Continuing Compliance	●	●
	.4 IdPO Risk Management	●	●
4.2.2 Registration and Identity Proofing	.1 RA Authentication	n/a	●
	.2 Identity Verification Process	n/a	●
	.3 Registration Records	n/a	●
	.4 Identity Proofing	n/a	●
	.4.1 Existing Relationship	n/a	●
	.4.2 In-person Proofing	n/a	●
	.4.3 Remote Proofing	n/a	●
	5. Address of Record Confirmation	n/a	●
	6. Protection of Personally Identifiable Information	●	●
4.2.3 Credential Technology	.1 Credential Unique Identifier	●	●
	.2 Basic Resistance to Guessing Authentication Secret	●	n/a
	.3 Strong resistance to Guessing Authentication Secret	n/a	●
	.4 Stored Authentication Secrets	n/a	●
	.5 Basic Protection of Authentication Secrets	●	n/a
	.6 Strong Protection of Authentication Secrets	n/a	●
4.2.4 Credential Issuance and	.1 Credential Issuance	●	●
	.2 Credential Revocation or Expiration	●	●

FICAM Updates 12/7/12 11:47 AM
Deleted: authentication

FICAM Updates 12/7/12 11:47 AM
Deleted: verification process

FICAM Updates 12/7/12 11:47 AM
Deleted: records

FICAM Updates 12/7/12 11:47 AM
Deleted: proofing

FICAM Updates 12/7/12 11:47 AM
Deleted: relationship

FICAM Updates 12/7/12 11:47 AM
Deleted: proofing

FICAM Updates 12/7/12 11:47 AM
Deleted: proofing

FICAM Updates 12/7/12 11:47 AM
Deleted: confirmation

FICAM Updates 12/7/12 11:47 AM
Deleted: unique identifier

FICAM Updates 12/7/12 11:47 AM
Deleted: guessing

FICAM Updates 12/7/12 11:47 AM
Deleted: guessing

FICAM Updates 12/7/12 11:47 AM
Formatted Table

FICAM Updates 12/7/12 11:47 AM
Deleted: issuance process

FICAM Updates 12/7/12 11:47 AM
Deleted: n/a

FICAM Updates 12/7/12 11:47 AM
Deleted: revocation

FICAM Updates 12/7/12 11:47 AM
Deleted: expiration

FICAM Updates 12/7/12 11:47 AM
Deleted: n/a

Functional Area	Criteria	Bronze	Silver
4.2.1 Business, Policy and Operational Criteria	1. InCommon Participant.	●	●
	2. Notification to InCommon	●	●
	3. Continuing Compliance	●	●
	.4 IdPO Risk Management	●	●
4.2.2 Registration and Identity Proofing	.1 RA Authentication	n/a	●
	.2 Identity Verification Process	n/a	●
	.3 Registration Records	n/a	●
	.4 Identity Proofing	n/a	●
	.4.1 Existing Relationship	n/a	●
	.4.2 In-person Proofing	n/a	●
	.4.3 Remote Proofing	n/a	●
Management	.3 Credential Renewal or Re-issuance	●	●
	.4 Credential Issuance Records Retention	n/a	●
	5. Resist Token Issuance Tampering Threat	●	●

Functional Area	Criteria	Bronze	Silver
4.2.5 Authentication Process	.1 Resist Replay Attack	●	●
	.2 Resist Eavesdropper Attack	●	●
	.3 Secure Communication	●	●
	.4 Proof of Possession	●	●
	.5 Session Authentication	●	●
	.6 Mitigate Risk of Credential Compromise	●	●
4.2.6 Identity Information Management	.1 Identity Record Qualification	●	●
4.2.7 Assertion Content	.1 Identity Attributes	●	●
	.2 Identity Assertion Qualifier	●	●
	.3 Cryptographic Security	●	●
4.2.8 Technical Environment	.1 Software Maintenance	n/a	●
	.2 Network Security	n/a	●

FICAM Updates 12/7/12 11:47 AM
Deleted: authentication

FICAM Updates 12/7/12 11:47 AM
Deleted: verification process

FICAM Updates 12/7/12 11:47 AM
Deleted: records

FICAM Updates 12/7/12 11:47 AM
Deleted: proofing

FICAM Updates 12/7/12 11:47 AM
Deleted: relationship

FICAM Updates 12/7/12 11:47 AM
Deleted: proofing

FICAM Updates 12/7/12 11:47 AM
Deleted: proofing

FICAM Updates 12/7/12 11:47 AM
Deleted: renewal

FICAM Updates 12/7/12 11:47 AM
Deleted: re

FICAM Updates 12/7/12 11:47 AM
Deleted: n/a

FICAM Updates 12/7/12 11:47 AM
Deleted: Retention of

FICAM Updates 12/7/12 11:47 AM
Deleted: issuance records

FICAM Updates 12/7/12 11:47 AM
Deleted: Page Break

FICAM Updates 12/7/12 11:47 AM
Formatted: Left, Indent: Left: 0"

FICAM Updates 12/7/12 11:47 AM
Deleted: replay attack

FICAM Updates 12/7/12 11:47 AM
Deleted: eavesdropper attack

FICAM Updates 12/7/12 11:47 AM
Deleted: communication

FICAM Updates 12/7/12 11:47 AM
Deleted: authentication

FICAM Updates 12/7/12 11:47 AM
Deleted: risk

FICAM Updates 12/7/12 11:47 AM
Deleted: compromise

FICAM Updates 12/7/12 11:47 AM
Deleted: record qualification

FICAM Updates 12/7/12 11:47 AM
Deleted: security

FICAM Updates 12/7/12 11:47 AM
Deleted: maintenance

FICAM Updates 12/7/12 11:47 AM
Deleted: security

	.3 Physical Security	n/a	●
	.4 Reliable Operations	n/a	●

FICAM Updates 12/7/12 11:47 AM
Deleted: security

FICAM Updates 12/7/12 11:47 AM
Deleted: operations

4.2 SPECIFICATION OF IDENTITY ASSURANCE REQUIREMENTS

This section contains all of the normative language for the Bronze and Silver IAPs.

In the requirements that follow, **(B)** indicates that the numbered section applies to the Bronze IAP; **(S)** indicates that the numbered section applies to the Silver IAP.

4.2.1 BUSINESS, POLICY AND OPERATIONAL CRITERIA

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

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.

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.

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.

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.

4.2.2 REGISTRATION AND IDENTITY PROOFING

Identity proofing in this IAP uses verified information to create a record for the Subject in the IdPO's IdMS.

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.

FICAM Updates 12/7/12 11:47 AM
Deleted: industry standard protocol

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.

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.

FICAM Updates 12/7/12 11:47 AM

Deleted: 3. Personally identifiable information collected as part of the registration process must be protected from unauthorized disclosure or modification.

FICAM Updates 12/7/12 11:47 AM

Deleted:

4.2.2.4 **(S)** 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:

4.2.2.4.1 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.

4.2.2.4.2 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.

FICAM Updates 12/7/12 11:47 AM
Deleted: it

4.2.2.4.3 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.

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.

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.

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.

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.

4.2.3.2 **(B)** BASIC RESISTANCE TO GUESSING AUTHENTICATION SECRET

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^{-10} (1 chance in 1,024) over the life of the Authentication Secret. This requires that an Authentication Secret be of sufficient complexity and, in most cases, that the number of invalid attempts to enter an Authentication Secret for a Subject be limited.

FICAM Updates 12/7/12 11:47 AM
Deleted:

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.

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.

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.

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

FICAM Updates 12/7/12 11:47 AM
Deleted: industry standard algorithm

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.

4.2.3.5 **(B)** BASIC PROTECTION OF AUTHENTICATION SECRETS

1. Authentication Secrets shall not be stored as plaintext. Access to stored Secrets and to plaintext copies shall be protected by discretionary access controls that limit access to administrators and applications that require access.
2. Plaintext passwords or Secrets shall not be transmitted across a network.

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.

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.

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.

4.2.4.2 **(S) (B)** CREDENTIAL REVOCATION OR EXPIRATION

1. The IdPO shall revoke Credentials 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.

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:

FICAM Updates 12/7/12 11:47 AM
Deleted: industry standard algorithms

FICAM Updates 12/7/12 11:47 AM
Deleted: and Tokens

FICAM Updates 12/7/12 11:47 AM
Formatted: Font:Bold, Raised by 1 pt

FICAM Updates 12/7/12 11:47 AM
Deleted: Appropriate policy and process must be in place to ensure that any new Credential and/or new Authentication Secret is provided only to the actual Credential Subject should it be necessary to reissue 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. ... [13]

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 are 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.

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.

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.

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.

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.

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.

4.2.5.3 **(S) (B)** SECURE COMMUNICATION

Communication between Subject and IdP must use a Protected Channel.

4.2.5.4 **(S) (B)** PROOF OF POSSESSION

The authentication process shall prove the Subject has possession of the Authentication Secret or Token.

4.2.5.5 **(S) (B)** SESSION AUTHENTICATION

If the IdP uses session-maintenance methods (such as cookies) so that after an initial authentication act new Assertions can be issued without the Subject having to re-authenticate, such methods shall use Approved Algorithms to ensure that sessions are at least as resistant to attack as initial authentication.

FICAM Updates 12/7/12 11:47 AM
Deleted: must…ay supply corre... [14]

FICAM Updates 12/7/12 11:47 AM
Formatted: Requirement, Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.63" + Indent at: 0.88"

FICAM Updates 12/7/12 11:47 AM
Deleted: 2. A short-lived single use Secret sent to the Address of Record that the Subject must submit in order to establish a new Authentication Secret. All interactions conducted via a shared network shall occur over a Protected Channel such as SSL/TLS. ... [15]

FICAM Updates 12/7/12 11:47 AM
Formatted: Font color: Auto

FICAM Updates 12/7/12 11:47 AM
Deleted: as defined in

FICAM Updates 12/7/12 11:47 AM
Formatted ... [16]

FICAM Updates 12/7/12 11:47 AM
Deleted: above

FICAM Updates 12/7/12 11:47 AM
Formatted: Font color: Auto

FICAM Updates 12/7/12 11:47 AM
Deleted: All interactions conducted via a network shall occur over a Protected Channel such as SSL/TLS.

FICAM Updates 12/7/12 11:47 AM
Deleted: records… record of Cre... [17]

FICAM Updates 12/7/12 11:47 AM
Formatted: Normal

FICAM Updates 12/7/12 11:47 AM
Deleted: unique identifier and the time of issuance/revocation

FICAM Updates 12/7/12 11:47 AM
Deleted: Industry standard cryptographic operations are required…ommunic... [18]

FICAM Updates 12/7/12 11:47 AM
Deleted: industry standard cryptographic techniques

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.

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.

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.

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.

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].

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.

4.2.7.3 **(S) (B)** CRYPTOGRAPHIC SECURITY

Cryptographic operations are required between an IdP and any SP. Cryptographic operations shall use Approved Algorithms.

FICAM Updates 12/7/12 11:47 AM

Deleted: industry standard cryptographic techniques

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.

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.

4.2.8.1 **(S)** SOFTWARE MAINTENANCE

IdMS Operations shall use up-to-date supported software.

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.

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.

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.

5 DETERMINATION OF CONFORMANCE

This section defines how an IdPO can determine conformance with the IAPs defined in this document and what supporting documents must be provided to InCommon when applying for certification.

5.1 CONFORMANCE WITH THE BRONZE PROFILE

An audit as defined in the inCommon IAAF may be done and documentation as described in the IAAF submitted at the time of application for InCommon Bronze certification.

Alternatively, the Participant may rely on the Representation of Conformance (RoC). The RoC includes a statement by the Participant that its IdPO is in conformance but does not require documentation of how that was determined. The RoC legally binds the Participant to remain in compliance as long as the Assurance Addendum to the InCommon Participation Agreement remains in force. The RoC must be submitted at the time of application for InCommon Bronze certification.

5.2 CONFORMANCE WITH THE SILVER PROFILE

An audit as described in the InCommon IAAF is required. Documentation as described in the IAAF must be submitted at the time of application for InCommon Silver certification.

5.3 CONFORMANCE WITH BOTH THE SILVER AND BRONZE PROFILES

Application for certification for both Silver and Bronze requires the audit as described above for Silver. That audit may include the Bronze IAP as well or either option described above for Bronze may be used.

APPENDIX A: REFERENCES

[IAAF] "**Identity Assurance Assessment Framework**", InCommon, version 1.1, 9 Apr 2011
http://www.incommon.org/assurance/

[InC-AtSum] "**InCommon Federation Attribute Summary**", InCommon Federation,
http://www.incommon.org/attributesummary.html

[TFPAP] "**Trust Framework Provider Adoption Process**", Federal Identity, Credential, and Access Management, Release candidate 1.0.1, 4-Sep-2009.
http://www.idmanagement.gov/

[SP 800-63] "**Electronic Authentication Guideline**", NIST, Special Publication 800-63-1
http://csrc.nist.gov/publications/PubsSPs.html

APPENDIX B: ACRONYMS

Acronym	Definition
IAAF	Identity Assurance Assessment Framework
IAP	Identity Assurance Profile
IAQ	Identity Assurance Qualifier
ICAM	Identity, Credential, and Access Management
ID	Identity Document
IdM	Identity Management
IdMS	Identity Management System
IdP	Identity Provider
IdPO	Identity Provider Operator
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
SP	Service Provider
TFPAP	Trust Framework Provider Adoption Process

APPENDIX C: 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.

Version 1.1 is an extensive revision to coordinate better with the [TFPAP].
Version 1.2 simplifies the Bronze Profile.

EDITORS

RL "Bob" Morgan	Tom Barton	David Walker
Jim Basney	Renee Shuey	John Krienke
Steven Carmody	Karl Heins	Ann West

Status	Release	Date	Comments	Audience
Public	1.0	4 Nov 2008	First full release for implementation	Open
Public	1.0.1	11 Mar 2009	Minor formatting fixes and clarifications	Open
	1.0.2	24 Mar 2010	Realignment of some criteria in prep for ICAM TFPAP	TAC
Public	1.0.3	22 Apr 2010	Updates for compliance with TFPAP	Open
Draft	1.1 D1	Dec 2010	Extensive revision	Limited
Draft	1.1 D8	24 Jan 2011	Further revision incl. consistent use of terms	Limited
Draft	1.1PRD1	9 Mar 2011	Revised from feedback and ready for larger review	Public
Draft	1.1FD1	9 Apr 2011	Revised from wider review; checked consistency, etc.	Limited
FINAL	1.1	9 May 2011	Approved by InCommon Steering Committee	Public
Draft	1.2v5	10 April 2012	Updated Bronze. Approved for community review by Assurance Advisory Committee	Limited
Public	1.2RC (Draft 6)	16 April 2012	Release Candidate Available for Public Comment	Public
Internal	1.2RCv8	17 May 2012	Clarified 4.2.5.6 refers to end-user credentials. Clarify intent of 4.2.1.4. Flag 4.2.2.5 to apply to Silver only.	Internal
Internal	1.2RCv8	22 May 2012	Approved by the InCommon Assurance Advisory Committee	Internal
Internal	1.2RCv9	8 June 2012	Removed process reference to align 5.1	Internal
FINAL	1.2	12 June 2012	Approved by InCommon Steering Committee	Public
Internal	1.2 rev 1	14 August	Changed "industry standard" to "Approved Algorithm"	FICAM

		2012	when referring to crypto techniques; updated 4.2.4.4 Credential Issuance Records Retention; updated 4.2.2.2.3.	
Internal	1.2 rev 4	30 November 2012	Recast 4.2.4.3. Included 4.2.4 as Bronze requirement; Clarified language.	FICAM