Defined Identity Assurance Program
Identity Assurance Assessment Framework

10/29/2008
Version 1.0

Executive Summary

The InCommon Federation maintains a registry of all Identity Providers that are recognized by the Federation. An InCommon Federation Identity Provider that wishes to offer identity assertions that meet a specific identity assurance profile under the InCommon Defined Identity Assurance program first must undergo an assessment of its identity management system against criteria that InCommon has defined. The InCommon Identity Assurance Assessment Framework describes the rationale for such an assessment and methodology that must be used in performing an assessment. The specific criteria to be used in the assessment process are not covered in this document; they are expressed in Identity Assurance Profiles as described in Section 2.

The initial Identity Assurance Profile document defines two profiles: "Bronze," which represents a basic level of assurance and "Silver," which adds stricter requirements. These profiles are intended to be at least compatible with the Federal government “Level 1” and “Level 2” identity assurance levels as described in NIST Special Publication 800-63 [SP 800-63]. Other profiles may be developed to meet the needs of other classes of service providers.

The assessment process results in one or more Identity Assurance Qualifiers that will be recommended to InCommon for this Identity Provider. The InCommon Federation Steering Committee has final authority over assignment of Identity Assurance Qualifiers to Identity Providers in the registry.

Registry information provided by InCommon describing an Identity Provider will indicate which Identity Assurance Qualifiers each Identity Provider is eligible to assert. The Identity Provider then may include the appropriate Identity Assurance Qualifier(s) in its own identity assertions. An InCommon Service Provider can make use of the presence or absence of such qualifiers in deciding whether to rely on identity assertions it receives.

This document is intended to help Identity Providers prepare for an assessment and inform auditors of the specific criteria to be examined. In addition, it may be used by a Service Provider or any other relying party that wishes to understand the trustworthiness of the binding between an identity Subject, identity credentials and identity assertions it might receive. This document also alerts those organizations to the necessary qualifications of auditors and how they should expect an auditor to evaluate assessments. Associated Identity Assurance Profile documents describe how to interpret criteria, and how to make judgments regarding findings.

It is expected that as the Identity Assurance Assessment Framework is used and the number of assessments undertaken increases, this document will evolve and be extended to reflect experience gained and additional needs of the InCommon community.

Table of Contents

1 INTRODUCTION

The InCommon Federation[1] for shared identity and access management provides operational and trust enhancement services to both Identity Provider (IdP) operators and Service Provider (SP) operators. Federation services increase efficiency by reducing redundant functions across Service Providers and by establishing common and consistent approaches to interoperable identity management. InCommon has established the Defined Identity Assurance (DIA) program in order to further achieve this efficiency through structured profiles of trusted identity intended to help mitigate risk to relying parties.

There are at least three parties to any federated identity transaction: the identity Subject (i.e., the identity credential user), the identity service operator (i.e., the IdP operator), and the relying party (i.e., SP operator). The identity Subject must trust the IdP operator to operate in a manner that supports reliable assertion of identity on behalf of the Subject while preserving his or her privacy. The IdP operator mitigates risk for the SP operator by minimizing the likelihood that another person would be able to claim that identity. Identity assertions offered by certified InCommon Federation Identity Providers may be relied upon across a wide range of Service Providers because the InCommon Federation articulates and verifies adherence to community standards for identity management and assertion through its DIA program as described in this Identity Assurance Assessment Framework (IAAF).

An Identity Provider operator may be an independent service organization or may be a functional unit that is part of a larger organization such as a university or commercial entity. The IdP operator registers Subjects in an identity management system (IdMS) and provides each Subject with a digital credential with which to identify herself or himself to the IdP while on-line. The IdP in turn provides appropriate identity information about that Subject to Service Providers that use it as part of managing access to their on-line resources. The InCommon Federation supports standards and infrastructure services to facilitate this set of transactions.

This document describes the IAAF and the rationale and processes involved in certifying an InCommon Federation IdP as capable of providing identity assertions that are backed by defined business and operational practices and credential technologies. These criteria include requirements for the identity-proofing of Subjects, digital credential technologies, and management of identity information used to make identity assertions. Many of the specific criteria are based on technical and policy guidance developed by the National Institute of Standards and Technology (NIST)[2]. They are intended to provide a structured means of defining assurances that should be meaningful to Service Providers that require well understood trustworthiness of a potential user's identity.

[1] See http://www.incommonfederation.org/

[2] See http://www.nist.gov/

The degree to which an IdP operator meets or exceeds requirements in these areas will determine which of the "Identity Assurance Profiles" (IAPs) that IdP operator is capable of supporting. Qualified IdP operators then can include the corresponding "Identity Assurance Qualifier" (IAQ) in identity assertions their IdP makes to SPs. SP operators that require assurance that an IdP can offer sufficiently trustworthy identity assertions should understand the InCommon DIA program and the IAAF and accompanying profiles and then determine which InCommon IdPs have been certified to provide the required identity assertion qualifier. The SP's then can check that identity assertions received actually contain the required identity assurance qualifier.

This is a normative specification. In order for an IdP operator to qualify as an InCommon Defined Identity Assurance, the processes described herein are mandatory, except for those sections that explicitly grant latitude or subjective judgment.

1.1 Related Documents

The reader should be familiar with the InCommon Federation Operating Policies and Practices (FOPP) and the InCommon Federation Participation Agreement. These may be found at http://www.incommonfederation.org/policies.cfm

The Federal Office of Management and Budget (OMB) "E-Authentication Guidance" [M-04-04] and NIST Special Publication "Electronic Authentication Guidelines" [SP 800-63] establish terminology and guidance for identity Assurance Levels and the technical requirements for Identity Providers that may offer identity assertions to Federal agency applications. InCommon has adopted compatible terminology, guidance and requirements.

OMB M-04-04 defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides Service Providers with the criteria for determining the level of authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence with each application or transaction. This document is available at http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

NIST Special Publication 800-63 provides technical guidance to Federal agencies implementing electronic authentication. The recommendation covers remote authentication of users over open networks. It defines technical requirements for each of four hierarchical levels of assurance in the areas of identity proofing, registration, tokens, system hardware, authentication protocols and related assertions. This document is available at http://csrc.nist.gov/publications/nistpubs/

These documents may be considered prerequisite reading for this IAAF document; it is assumed the reader is familiar with the concepts they establish.

The specific criteria used to assess Identity Providers are grouped into Identity Assurance Profiles which are described in Section 2. The initial IAP defines profiles for InCommon Bronze and InCommon Silver qualification. Additional profiles may be defined as needs arise.

The IAAF, Bronze and Silver IAP, and NIST Password Entropy Spreadsheet currently comprise the InCommon Defined Identity Assurance document suite. The complete document suite is maintained on the InCommon Federation website, and is available at https://spaces.internet2.edu/display/InCCollaborate/InCommon+Identity+Assurance

1.2 General Approach

As the federation operator, InCommon serves an important role by certifying that IdP operators conform to adopted standards for identity assurance and may be trusted, consistent with community expectations. This section provides a general overview of the approach that InCommon takes toward providing this service.

The InCommon Federation maintains a registry of all IdPs that are recognized by the Federation and provides information from that registry to InCommon SPs. Those IdP operators that wish to offer assurance qualified identity assertions must demonstrate that their identity management processes meet criteria defined by InCommon. The required criteria are presented in Identity Assurance Profiles (IAPs) further described below. If found to conform with the requirements of one or more profiles, the IdP operator is allowed to assert the appropriate Identity Assurance Qualifier (IAQ) in identity assertions it offers.

Any SP participating in InCommon can make use of identity assertions from any IdP in the registry. However, it is strongly recommended that SP operators assess potential risks associated with access to their resources using an industry accepted risk assessment methodology and then require that an IdP's certified Identity Assurance Qualifier indicate conformance with an identity assurance profile sufficient for the particular application.

The first step for an IdP to be certified to assert one or more IAQs is for the IdP operator to perform an assessment of its identity management policies, practices and processes and controls against the requirements in the appropriate IAP(s). Once complete, the IdP operator then must engage an information technology (IT) auditor, such as a Certified Information Systems Auditor[3] (CISA) who is familiar with information technology security issues to perform an audit of the IdP's assessment and relevant controls. The selected auditor must be sufficiently independent from the functional unit that supports the service being assessed.[4] The audit must cover all the specific criteria defined in each applicable IAP. The evidence used to make the assessment is verified by the auditor and used to evaluate compliance. Any criteria which are not met may be corrected by the IdP and then re-examined by the auditor until compliance is achieved or it is determined that compliance is not possible. Alternatively, the auditor may declare that an IdP operator's practices, although different from those defined in the IAP, meet or exceed the intent of the specific IAP requirement(s). Once certified, IdP operators are required to undergo periodic reassessments, as defined in the IAP, to verify continuing conformance with IAPs under which they have been certified.

[3] See Information Systems Audit and Control Association `http://www.isaca.org/`

[4] See section 3.1 below.

When the audit is complete, the auditor writes a letter[5] to InCommon that summarizes results of the assessment and audit. InCommon reviews the letter and makes the final determination regarding assignment of an IAP designator to the IdP in the InCommon IdP registry. For those IdPs that meet the criteria, InCommon then adds the appropriate designator(s) to the IdP's registry entry. The IdP then may include one or more of its certified IAQ(s), as appropriate, in identity assertions that it provides to SPs.

A given IdP operator may support a diverse community of Subjects and may have somewhat 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 all faculty and for staff that perform in management roles that require it. A campus IdP operator might support "guest accounts" for visitors for which there is no formal identity assurance and hence no applicable IAP or IAQ. 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 appropriate IAQ in identity assertions for that Subject. An InCommon IdP 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.

It is a responsibility of the IdP operator, as defined in the DIA Addendum to the InCommon Participation Agreement, never to assert knowingly an identity assurance qualifier to an InCommon SP that has not been assigned to the IdP by InCommon and to ensure that any IAQ that is asserted is appropriate for the particular identity assertion being offered.[6]

[5] See section 3.2.1 below.

[6] The protocol and technical implementation for conveying identity assurance qualifiers is described in ???

2 IDENTITY ASSURANCE PROFILES

An InCommon Identity Assurance Profile specifies a set of criteria that, if met or exceeded by an IdP operator, allow an SP to determine whether identity assertions conforming to those criteria can be used to help manage access to its service(s). Sufficient assurance of an identity may involve many factors including registration of a Subject in an identity management system, the type of digital credential provided to the Subject, the management of identity information about the Subject, and the security of the processes used to provide an identity assertion. Identity Assurance Profiles reflect industry and/or government consensus regarding requirements and best practices in each relevant area and may change or evolve over time.

IAPs are developed to be useful for general classes of on-line SPs. For example, some SPs require only a unique identifier for each Subject while other SPs require only group affiliation. Some SPs require strong assurance of the binding between the Subject and any identity information offered by the IdP. Some SPs may require a rich set of identity information about Subjects. Each IAP will include all factors that contribute to the security, reliability and accuracy of an identity assertion, as discussed below. The specific criteria and requirements are defined in InCommon IAP documents.

InCommon IAPs are not necessarily hierarchical in nature. They merely represent different sets of identity management practices and requirements. In some cases, an IdP operator conforming with a given IAP may also thereby conform with another, less strict IAP. This is the case with InCommon Bronze (see below) which is a subset of InCommon Silver. Thus an IdP operator qualifying for InCommon Silver need not also formally apply for qualification at InCommon Bronze; this latter qualification is a consequence of the former.

No InCommon IdP operator is required to qualify under any of the defined IAPs. InCommon IdP operator Participants only are required to self-describe their identity management practices and make that statement available to InCommon SPs.[7] This "self-described" IAP might be considered 'higher education institution common practices identity assurance.' Identity assertions provided solely on the basis of this self-described profile must not contain any InCommon identity assurance qualifier (IAQ).

2.1 InCommon Defined Identity Assurance Services Profiles

The initial InCommon IAP document establishes requirements for IdP operators under two assurance profiles: "Bronze," which represents a basic minimal set of requirements and "Silver," which adds more stringent requirements. InCommon Bronze and Silver are intended to be compatible with Federal NIST 800-63 Levels 1 and 2. Silver also includes criteria regarding support for InCommon eduPerson basic identity attributes. Future IAPs may cover richer identity sets and/or may be designed for different classes of services.

[7] See the InCommon POP requirements at http://www.incommonfederation.org/policies.cfm

2.1.1 InCommon Bronze Identity Assurance Profile

The InCommon Bronze identity assurance profile focuses on sequential identity (reasonable assurance that the same person is authenticating each time) and group identity (reasonable assurance that the person authenticating is a member of a defined group known to the IdP operator). Authentication assertions under this profile are likely to represent the same Subject each time a Subject identifier[8] is provided. Group attributes such as "affiliation" or "entitlement" are likely to be accurate.

The Bronze profile should be sufficient for managing access to services and resources for which risks due to incorrect identification of the Subject are minimal, specifically neither financial loss nor harm to persons or property. Since only minimal assurance of personal identity is provided so this profile may not be sufficient when personal responsibility for actions is required. Determination of applicability for any particular use is a responsibility of the SP.

While no identity proofing requirements are specified, it is expected that IdP operators use reasonable care when issuing authentication credentials to confirm that a single individual applies for and receives a given credential *and* its "shared secret" or similar credential verifier. Campuses are expected to issue such credentials to individual students, faculty, and employees that would be sufficient to protect campus academic information and intellectual property resources.

InCommon Bronze qualified identity assertions should be usable by individuals seeking access to on-line information resources licensed to an organization of which the Subject is an eligible member, and to on-line services where the SP will invoke "knowledge based" linking of the Subject identifier to information the SP already has regarding individuals who should have access to its services.

In general, InCommon Bronze qualified identity assertions may be trusted by an SP where the consequences of an authentication error are tolerable by the SP.

2.1.2 InCommon Silver Identity Assurance Profile

The InCommon Silver identity assurance profile builds on the Bronze profile requirements adding criteria regarding business processes, individual Subject identity proofing, and identity information management. Stronger credential technology and credential management is required as well. This assurance profile should be sufficient for applications that require individual user accountability but for which risk is still limited.

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 identity assertions. Per the NIST 800-63 Level 2 requirements, digital authentication credentials must at a minimum make use of reliable "shared secret" technology such as a userID and a password that is sufficiently difficult to guess or intercept. Stronger credential

[8] The principle Subject identifier might change for a given individual but a given identifier should not be reassigned to represent a different individual for a defined period of time after it has been deprecated. It must be safe to use such an identifier in an Access Control List (ACL) and not risk inappropriate access by a different Subject.

technologies such as Kerberos or PKI smartcards should be acceptable as long as their issuance and management meet or exceed requirements in the Silver IAP.

Information in identity assertions offered by an IdP to an SP under the Silver IAP should be reasonably accurate but there are no specific requirements that must be met. A Silver certified IdP operator should support at least the InCommon basic eduPerson identity attributes.

An IdP operator that qualifies under the Silver IAP is automatically qualified under Bronze as well.

2.2 Assessment Criteria

Assessment criteria in the following areas and issues of relevance will be defined in each IAP, as appropriate. Not all criteria will appear in every profile; only those relevant to the profile will be defined. Assessors must understand these criteria and be qualified to evaluate identity management systems to determine compliance.

2.2.1 Business, Policy and Operational Factors

An InCommon IdP operator and each of its identity services must be trustworthy and reliable as an entity in order to offer reliable identity services. Such an IdP operator must be a legal entity, or part of a larger organization that is a legal entity, in order that it can enter into contracts with other legal entities and accept liability for its actions. It must have adequate resources and infrastructure to support the services it offers.

Issues and criteria to be addressed include:

- Is the IdP operator an independent legal entity or is it part of a larger organization that is a legal entity? Does it have a charter or clear authority from the parent organization to offer the identity services it claims to support?
- Does it have adequate written business policy and practices, including information security policy and technical security practices? How is adherence assured?
- Can it demonstrate sufficient maturity in operating its services?
- Does the IdP operator have a Business Continuity Plan and is it prepared to respond to and recover from an emergency or interruption of service?
- Does it retain business and operational records sufficiently for problem resolution, forensic analysis, and to meet legal and regulatory requirements?
- Is there an Identity Subject Agreement requiring, among other things, protection of shared secrets and notification to the IdP operator of changes to the Subject's identity profile?

2.2.2 Registration and Identity Proofing

Identity proofing is the process by which an IdP operator or its Registration Authority (RA) correctly associates a particular physical person with an existing identity information record in the IdP operator's Identity Management System (IdMS) repository or directory, or gains the personal information required to create a new record for that physical person.

If the IdP operator is part of a larger organization then identity Subjects that are associated with that organization (e.g., employees and/or students), may have undergone the required identity proofing during the process of bringing each person into the larger organization. However, if the IdP operator is an independent provider of identity services, then the Subject must provide one or more authoritative documents, which should be verified by the IdP operator, in order to ensure a reliable repository or directory record association or to initiate a new, unique record for that Subject.

During identity proofing, sufficient information must be acquired to enable the IdP operator to contact the Subject or, in some cases, locate the physical Subject if necessary. In some profiles, a record of the authoritative documents presented by the Subject must be retained as well to show proof of process or to aid in re-establishing an identity association at a future time.

Issues and criteria to be addressed include:

- IdP operator personnel security requirements
- In-person versus other processes such as remote proofing, proxy proofing, knowledge-based processes, etc.
- Organizational identity based on established relationship versus independent identity service provider
- Documents or data feeds required to establish the Subject's binding to his or her IdMS record
- Retention of records of the identity proofing process

2.2.3 Digital Electronic Credential Technology

A digital electronic credential is the means by which an identity Subject authenticates to a given IdP. The "strength" of this credential - the likelihood of misuse or spoofing of the credential - is a primary factor in determining the trustworthiness that an identity assertion might have. For shared secret credentials, e.g., userID/password, the "secret" must be sufficiently difficult for a different person to "guess" and must be protected from illicit capture or replay. Physical token-based credentials must be resistant to misuse if lost or stolen. The NIST document referenced in section 4 provides guidance on the strength of various digital electronic credential technologies.

In some cases a given Subject might have more than one credential to accommodate different authentication scenarios. For example, when traveling, a Subject might use a userID and password to authenticate but when at work a smartcard might be required. Another example is use of a userID and password to authenticate for general services but requiring a Subject to provide a second authentication token when she or he attempts to access administrative systems. Other factors might be significant such as location of the Subject (e.g., on the campus network or on some remote network). Thus identity assertions on behalf of each Subject might fall under different profiles depending on the type of authentication credential and method that was used and other factors. Similarly, if the IdP operator is aware of a possible compromise of a Subject's credential, it might be required to assert a different IAQ or suspend or invalidate the credential until the concern is resolved.

Re-authentication of the Subject by the IdP's credential system verifier might be required by some SPs if the current authentication event occurred too long in the past[9]. With some credentials, e.g., smartcards, this requirement implies a built-in timeout in the Subject's device. If such re-authentication is required by an IAP, it may limit the types of digital credentials that can be supported by the IdP operator.

Issues and criteria to be addressed include:

- The type of credential and verification model used
- How resistant shared secrets are to guessing, e.g., the entropy required of passwords
- Whether shared secrets are ever exposed to potential interception
- The IdP operator's response to authentication failure or suspicious activity
- The ability to re-authenticate the Subject when necessary

2.2.4 Digital Electronic Credential Issuance and Management

The purpose of the digital credential is to associate the holder with a particular IdMS record. As such, the credential will contain an identifier unique to that IdMS record. That identifier may or may not be used as the Subject's identifier in identity assertions to SPs. In general, it would be good practice to use a different identifier for those two purposes so that each identifier could be structured appropriately or a new credential could be issued to the same Subject or the same Subject could be issued a new external identifier.

It is important to note that registration, identity proofing, and token and credential issuance represent different goals of the same process. In many cases, however, this process may be broken up into a number of separate physical encounters and electronic transactions. (Two electronic transactions are considered to be separate if they are not part of the same protected session.) In these cases, methods should be used to ensure that the same party acts as Applicant throughout the entire process.

Creating and conveying an identity credential to a Subject must ensure that the Subject actually receives the credential and has control of the credential authentication secret, i.e., "shared secret" or PIN. It also should minimize the possibility that some other person might acquire the authentication secret during the process. Credentials that are forgotten or about to expire and must be reissued, if appropriate, must be handled in a similarly secure manner. Credentials that are no longer needed or have been compromised must be invalidated in a timely manner.

A credential for which the authentication secret has been lost or is suspected of having been compromised should decrease the overall assurance of an identity assertion. Such a credential may be restored by allowing the Subject to select a new authentication secret (PIN or password). The process for this should be as secure as the original credential issuance process but it could be based on significant unique knowledge that only the Subject and the IdP operator possess.

A credential that might expire may be renewed by the Subject if there is no reason to

[9] See section 2.2.5 below.

believe the authentication secret has been compromised or the Subject's basic information has changed.

Issues and criteria to be addressed include:

- How the credential is created
- How the credential and its authentication secret are delivered to the Subject
- Process for confirmation that the Subject has control of the authentication secret
- Management and protection of the authentication secret when used by the IdP's credential verification process
- Procedures for reporting and invalidating a compromised credential
- Procedures for invalidating a credential that is no longer needed, e.g., because the Subject is no longer associated with the IdP operator or organization
- Procedures for re-issuing an expired or invalidated credential

2.2.5 Security and Management of Authentication Events

An authentication event occurs when a claimant offers his or her credential to an IdP's credential verifier, the verifier interacts with the claimant to confirm he or she is the rightful physical person associated with authentication credential, and the verifier checks that the credential is still valid (i.e., neither suspended nor invalidated nor expired). This transaction must be secure against interception or exposure of any authentication secret. The time, date, and nature of the authentication event should be recorded and may be requested as part of identity assertions.

Some SPs may wish to request recurrence of the authentication event where the most recent event occurred too long in the past. If this capability is supported by the IdP, the SP can decide whether or not to confirm that the identified Subject is still in control of the current session.

Issues and criteria to be addressed include:

- How authentication events are secured
- What logging occurs and how long it is kept
- Whether authentication event details can be included in an identity assertion
- Whether re-authentication can be requested for a given Subject

2.2.6 Identity Information Management

Identity assertions offered by the IdP to an SP will be based on information about or pertinent to the identity Subject, e.g., "name" or "unique identifier." Management of the identity information repository or directory that stores this information is critical to the degree of assurance that an assertion might carry. Not only must the repository or directory be secure and robust but identity information must be updated when appropriate and updates must be verified and carried out by trustworthy individuals.

Information about a Subject must be reasonably authoritative or should be marked

otherwise.[10] For example, an employer could properly assert the employment status of its employees but should only assert as "self identified" a Subject's membership in an unrelated recreational organization. In some cases, identity information may be acquired from a third party, e.g., another campus or a professional organization. Such information may be authoritative if it is acquired in a secure manner from an authoritative source but in other cases may be merely advisory. IdPs should not convey attribute information of any type as authoritative unless it can be shown to be so.

Some identity information used in assertions to SPs may be defined in a profile. It is not necessary that all such information be part of a profile. IdPs may offer additional information as needed by an SP. However, only the information defined in a profile can be assumed to be assured under the profile referenced by an IAQ. The reliability of any other information is undefined unless there is a separate agreement between the parties.

Abstract identifiers[11] generated for an IdP operator's Subjects may be used by SPs to manage access. For this reason such identifiers must be unique among all of the IdP operator's Subjects and must not be reassigned, at least for some period of time, after a Subject is no longer associated with a particular identifier. A given Subject may have any number of abstract identifiers but a given identifier must map only to a specific Subject. Abstract identifiers need not be persistent over time, i.e., they can be removed from use.

Identity information about a Subject should be obtained from an authoritative Office of Record. An IdP operator that is part of a larger organization, or that is providing identity services under contract to an organization, should have a written agreement in place for the acquisition, storage, and use of authoritative information about Subjects.

Transfer of authoritative information from the Office of Record to the IdP operator's IdMS should use security methods to prevent unauthorized modification of the data. Digitally signed files and/or secure communication channels should be used.

Subject identity information should be kept up to date. Changes may be initiated by the Subject or by the Office of Record. The process of updating the IdMS database should be secure against unauthorized changes or modification, including partial or complete destruction. Write and modify access should be managed by credentials at least as trustworthy as the most trusted credentials issued by the IdP operator.

All actions that affect the integrity or contents of the IdMS database should be logged securely and in a manner that is resistant to tampering.

Issues and criteria to be addressed include:

- Documentation of the IdP operator's identity management processes and operations
- Processes for ensuring that a unique identifier is unique, protected and not reassigned
- Processes for Subject data acquisition, verification and change management
- Generation and management of other Subject information, e.g., entitlement, etc.
- Termination of inactive Subject access

[10] Until a way to accomplish this in practice is defined, only authoritative information should be asserted.

[11] An identifier carrying no other information or semantics.

2.2.7 Identity Assertion Content and Subject Consent

Identity information about an individual that an InCommon Federation IdP might convey to a relying party is referred to as a set of "attributes" - structured, named information objects that refer to or pertain to the identity Subject. Identity attributes as used by InCommon are described on the InCommon Federation Attribute Overview web page. Specific attributes recommended for use by all IdPs[12] and SPs are a described on the InCommon Federation Attribute Summary web page. Other attributes may be added to list from time to time. The actual meaning of any attribute values identified as recommended for use by InCommon Participants must be consistent with the definitions in the most recent InCommon document. Any other attributes used from the eduPerson object class must have the meaning described in the eduPerson specification.

InCommon IdP operators conveying any of these attributes must ensure that the meaning of such information conforms with the InCommon definitions for these objects. The IdP operator should include in assertions only those attributes that it acquires from authoritative sources and stores securely.

Other identity attributes of use to SPs and known authoritatively by the IdP operator may be offered in assertions provided that the names and/or OIDs for those attributes do not conflict with those defined for use by InCommon. Such attributes should be given names and OIDs that are distinct from InCommon's or any other IdP operator's unique attributes.

IdPs should convey to SPs only those attributes that are required or a default set if specific requirements are unknown. In some cases, identity Subjects should be able to determine what additional attributes will be conveyed to a particular SP.

Identity Subjects should be able to block release of certain identity information to one or more Relying Parties even if that might mean they are denied service as a result. In addition, members of some classes of persons, e.g. "students", may be covered by legislation or regulation[13] that requires prior approval for release of certain information.

Issues and criteria to be addressed include:

- Documentation of how identity attributes conform to InCommon-approved definitions
- What identity information is available for assertions
- How Subjects might control the release of their identity information
- How privacy of a Subject's information is protected

2.2.8 Technical Environment

IdP operators must implement technology in conformance with InCommon technical requirements and must be able to demonstrate interoperability with reference implementations. They must be willing to participate in problem resolution both with technology and with identity assertion anomalies. IdP operators must operate in a secure

[12] If appropriate; see paragraph 1.3.3.

[13] Specifically now in the European Union.

network environment and with security controls and procedures in place for all identity management systems. [ISO/IEC 27001/2] as well as Federal government documents [FIPS 199], [FIPS 200], and NIST [SP 800-53] provide relevant guidance in these areas. Other standards may apply.

All service platforms involved in delivery of the IdP operator's services including registration, identity database, or identity assertion processing should have appropriate firewalls installed and active and should be kept up to date with security-related software patches.

Cryptographic keys used for signing of identity assertions should be protected against unauthorized use.

To the extent possible, the IdP service's system architecture should be resistant to denial of service attacks.

IdP operators should provide for continuity of identity verification and assertion services in case of system failures or natural disasters. Minimizing single points of failure, providing backup or stand-by service platforms and replicating critical data to off-site locations are good practices.

Issues and criteria to be addressed include:

- Network and platform security measures in effect
- Demonstration of technical interoperability
- Processes for problem resolution
- Provisions for backup and disaster recovery

3 ASSESSMENT AND AUDIT OF IDENTITY PROVIDERS

As described above, InCommon IdP operators that wish to participate in the DIA Program must undertake initial assessment and then arrange for an independent audit of that assessment, and, for some IAPs, periodic re-assessment and audit of the controls for their identity and credential management systems. InCommon neither initiates nor performs such assessments or audits. The Auditor must provide the report required by InCommon and should send it directly to InCommon. It is highly recommended that such IdP operators contact InCommon before initiating this process to confirm that the most up-to-date documents and criteria will be used.[14]

3.1 Auditor Qualifications

The Auditor may be either an external contractor or may be a member of an internal audit office within the IdP operator's parent organization. The Auditor doing the review must be objective and independent of the IdP's organization following guidelines established by professional audit organizations such as The Institute of Internal Auditors *Standards for the Professional Practice of Internal Auditing.*

The Auditor shall possess adequate technical proficiency and industry knowledge for the specific assessment being performed. The Auditor must have demonstrated qualification to make competent determination of the Identity Provider's services compliance with applicable IAP criteria, taking into account technical issues and specific requirements that the criteria might set out (e.g., specific management processes). The Auditor shall have, as a minimum:

- Understanding of the IdP operator's industry and services;
- Knowledge of the specific technologies/techniques being assessed;
- Technical and management audit experience;
- Familiarity with this IAAF Suite and its principles.

To audit an IdP operator under the Silver IAP, the Auditor must have current direct experience as an information technology auditor. Demonstrated qualifications, such as designation as a Certified Information System Auditor or equivalent is required.

3.1.1 Subjective Judgment

Auditors may be required to exercise a degree of subjective judgment when testing the assessment of the IdP operator and its service(s). Despite the structure of the IAAF and its associated IAPs, Auditors may have to rely on their experience and domain knowledge when determining an IdP operator's compliance with specific criteria. Departures from normal procedures or requirements must be documented in the Auditor's report to the IdP operator, and may be made available to InCommon. Documentation should include the IdP operator's rationale for such departures.

[14] Contact `incommon-admin@incommonfederation.org`

3.2 Audit Report

The Auditor must prepare a written audit report to document the approach, findings, and recommendations regarding compliance of the IdP operator with specific IAP(s). Audit reports should be delivered to the highest level manager of the IdP operator. An audit report must include:

- Assessment Objective. The Auditor must identify the IdP operator, its organizational structure and, if relevant, its placement within a parent organization, and the identity profile(s) that the IdP operator wishes to support;
- Scope and Methodology. The IdP operator's organization must provide full and unrestricted access to all records, people and processes. The scope of the review should include sufficient tests of controls identified in the InCommon IAP to render an appropriate opinion; and
- Findings. The Auditor must report the IdP operator's compliance with each of the criteria contained in the relevant IAP(s). For each criterion, the Auditor should identify the evidence provided, the rationale for acceptance or rejection, and any identified deficiencies. If significant vulnerabilities are found, e.g., in security or operational controls, these should be resolved in discussions with the IdP operator and the report should not be finalized until they are corrected or mitigated sufficiently.[15] The audit report shall identify the Auditor, it's basis for independence with respect to the IdP operator, and the dates during which the audit took place.

3.2.1 Conveyance to InCommon

A signed copy of the final audit report should be conveyed directly to InCommon by the Auditor. However, if the IdP operator has concerns about sharing sensitive or proprietary information about it's operations, the Auditor must prepare and sign a letter to be conveyed to InCommon summarizing the final assessment results. The letter must as a minimum:

- identify the Auditor, including qualifications;
- outline the audit methodology;
- identify any points where alternatives to IAP requirements were deemed satisfactory;
- state whether the IdP operator conforms with the requirements of each IAP considered.

All audit reports and letters will be kept in strict confidence by InCommon. The InCommon Steering Committee will address any questions that may arise about an IdP operator's audit report.

3.3 Changes to the Identity Provider Operation

The IdP operator must notify InCommon of any material changes (i.e., changes to evidence of status from compliant to non-compliant) by the IdP operator that may affect its qualification under an IAP. Notification should occur 60 days before the changes are to be made effective, or as soon as practicable after an unanticipated change is noted. InCommon will determine whether the changes are sufficient to require re-assessment.

[15] InCommon will keep such information confidential.

Any change-driven re-assessment would only need to cover those elements that have changed.

Additional maintenance activities may be stipulated in the DIA Addendum to the InCommon Participation Agreement between InCommon and the IdP operator's organization.

3.4 Identity Provider Qualification Certification

Once the IdP operator is certified by InCommon to operate under one or more IAPs, InCommon Operations will place the appropriate identity assurance designator(s) in the IdP registry entry describing the IdP. SPs and other parties will acquire this information as part of their next InCommon participant refresh cycle.

4 REFERENCES

[ANSI X9.31] "**Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry**", American National Standards Institute, 1998

[ISO/IEC 27001/2] "**Information Security Management Systems Requirements / Code of Practice for Information Security Management**" Jun 2005

[FIPS 140] "**Security Requirements for Cryptographic Modules**", NIST Federal Information Processing Standards, http://csrc.nist.gov/publications/PubsFIPS.html

[FIPS 199] "**Standards for Security Categorization of Federal Information and Information Systems**", NIST Federal Information Processing Standards, Feb 2006, http://csrc.nist.gov/publications/PubsFIPS.html

[FIPS 200] "**Minimum Security Requirements for Federal Information and Information Systems**", NIST Federal Information Processing Standards, Mar 2006, http://csrc.nist.gov/publications/PubsFIPS.html

[M-04-04] Federal OMB "**E-Authentication Guidance for Federal Agencies**", Dec 2003, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[RFC 3280] "**Internet X.509 Public Key Infrastructure**", IETF, April 2002, http://www.ietf.org/rfc/rfc3280.txt?number=3280

[RFC 5246] "**The Transport Layer Security Protocol**", IETF, August 2008, http://www.ietf.org/rfc/rfc5246.txt?number=5246

[SP 800-53] "**Recommended Security Controls for Federal Information Systems**", NIST Special Publication 800-53, December 2006 http://csrc.nist.gov/publications/nistpubs/

[SP 800-63] "**Electronic Authentication Guidelines**" NIST Special Publication 800-63 http://csrc.nist.gov/publications/nistpubs/

[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

Appendix A: Glossary

Term	Definition
Active Attack	An attack on the authentication protocol where the attacker transmits data to the claimant or verifier. Examples of active attacks include a man-in-the-middle, impersonation, and session hijacking.
Address of Record	The location where an individual can be found to best knowledge of the IdP operator. If this information is going to be included in an identity assertion, it must be verified by the IdP operator via registered US mail. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available.
Approved	NIST recommended. An algorithm or technique that is either 1) specified in a NIST Recommendation, or 2) adopted in a NIST Recommendation. Approved cryptographic algorithms must be implemented in a crypto module validated under [FIPS 140]. For more information on validation and a list of validated FIPS 140-2 validated crypto modules see http://csrc.nist.gov/cryptval/
Attack	An attempt to obtain an identity Subject's token or to fool a verifier into believing that an unauthorized individual possess a claimant's token.
Attacker	A party who is not the claimant or verifier but wishes to successfully execute the authentication protocol as a claimant.
Assertion	A statement from a IdP to a relying party that contains identity information about a subscriber. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol.
Assurance Level	Level of trust, as defined by the OMB Guidance for Federal government E-Authentication [M-04-04]. This guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four levels of assurance are: Level 1: Little or no confidence in the asserted identity's validity. Level 2: Some confidence in the asserted identity's validity. Level 3: High confidence in the asserted identity's validity. Level 4: Very high confidence in the asserted identity's validity.
Assurance Profile	See Identity Assurance Profile.

Authentication	The process of verifying a binding between a physical person and an identifier uniquely assigned to that person and presented in a digital electronic credential. Verification requires that the person also present one or more of • something they know, e.g., a secret or other special knowledge • something they have possession of, e.g., a smartcard, etc. • something they are, as represented by a biometric measurement.
Authentication Event	An instance of the process of receiving a credential, verifying that the claimant has possession of the credential authentication secret, and verifying that the credential is still valid.
Authentication Protocol	A well specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.
Authentication Secret	Something that only the claimant should possess (typically a private key, PIN or password) used to verify the claimant's use of his or her credential to claim an identity.
Authentication Service Component	Interface specifications that describe the requirements for IdP services to technically interoperate with Relying Parties. See http://www.incommonfederation.org/technical.html
Challenge-Response Protocol	An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (either cryptographically or by hashing the challenge and secret together) to generate a response that is sent to the verifier. The verifier knows the shared secret or decryption key and can independently compute the response and compare it with the response generated by the claimant. If the two are the same, the claimant is considered to have successfully authenticated himself. When the shared secret is a cryptographic key, such protocols are generally secure against eavesdroppers. When the shared secret is a password, an eavesdropper does not directly intercept the password itself, but the eavesdropper may be able to find the password with an off-line password guessing attack. An example of this is the "proof of possession of the Private Key" during a PKI certificate verification interchange.
Claimant	A party whose identity is to be verified using an authentication protocol.
Credential	The publicly sharable token or document that a claimant offers in order to assert an identity.
Cryptography	The discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof. [ANSI X9.31] Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption.
Cryptographic Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, keys must provide at least 80-bits of protection. This

	means that it must be as hard to find an unknown key or decrypt a message, given the information exposed to an eavesdropper by an authentication, as to guess an 80-bit random number.
Cryptographic Module	The set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
Digital Signature	An asymmetric key operation where the private key is used to create an encrypted representation of an electronic document and the public key is used to verify that the original document has not been changed. The holder of the private key is assumed to be responsible for creating the digital signature. Digital signatures therefore provide a means for authentication and integrity verification of digital documents.
Digital Credential	A digital electronic document used in authentication that binds the credential holder to an identifier and/or identity information. The Claimant also must verify that he or she holds an authentication secret, e.g., password, PIN, etc., in order for the credential to be considered trustworthy by a relying party.
Eavesdropper	Refers to any device or person that intercepts or copies an electronic transmission.
Electronic Digital Credential	See Digital Credential.
Entropy	A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits. Guessing entropy is a measure of the difficulty that an attacker has to guess the average password used in a system. In this document, entropy is stated in bits. When a password has n-bits of guessing entropy then an attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The attacker is assumed to know the actual password frequency distribution.
FIPS 140-2	Specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The FIPS 140-2 standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.3 d) FIPS 140-2 shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract.
Guessing Entropy	A measure of the difficulty that an attacker has to guess the average password used in a system. In this document, entropy is stated in bits. When a

	password has n-bits of guessing entropy then an attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The attacker is assumed to know the actual password frequency distribution.
Hash-based Message Authentication Code (HMAC)	Hash-based Message Authentication Code: a symmetric key authentication method using hash functions.
Identity	The set of true information that correctly pertains to a physical person or other entity. Some information is unique, e.g., DNA; some information is shared with other entities, e.g., "student" or "politician. Pseudonymous identifiers might be part of a person's identity, used to protect his or her personally identifying information while offering unique binding to that specific person. The particular identity information that is relevant in any transaction depends on the nature and context of that transaction.
Identity Assurance Profile (IAP)	A set of requirements and criteria that help a relying party determine the trustworthiness and/or usefulness of an identity assertion. Profiles can be created for different types of applications or uses. An IdP operator can be qualified to provide assertions that meet or exceed the stipulations of one or more Profiles.
Identity Assurance Qualifier (IAQ)	An element added by a qualified IdP to an identity assertion to indicate that the assertion was created in compliance with the specific InCommon Identity Assurance Profile. An assertion may contain more than one IAQ.
Identity Federation	A set of otherwise independent identity providers and relying parties that agree to adhere to common rules and requirements for identity management and the use and protection of identity information.
Identity Proofing	The process by which an IdP operator and/or an RA verify sufficient information to uniquely associate a physical person with a record in the IdP operator's IdMS. A new IdMS record may be created for the Subject if no match is found to a previously existing record.
Identity Provider (IdP)	The software and hardware that make use of an IdMS to provide identity information, e.g. identity assertions, to Relying Parties, typically Service Providers (SPs). An IdP operator may support more than one IdP service.
IdP operator	A trusted organization or functional unit that issues or registers identity Subject tokens, issues electronic credentials to identity Subjects, and provides identity information to Relying Parties on behalf of identity Subjects. The IdP operator may encompass Registration Authorities and credential verification systems that it operates. An IdP operator may be part of a larger entity that requires such a service. An IdP operator may outsource part of its functions e.g., credential issuance and management, to an independent third party. An IdP operator may offer more than one type of credential or IdP service. An IdP operator that participates in an identity federation may be certified by that federation with respect to how its operations compare with

	established federation standards.
Impractical	"Impractical" is used here in the cryptographic sense of nearly impossible, that is, there is always a small chance of success but even the attacker with vast resources will nearly always fail. For off-line attacks, impractical means that the amount of work required to "break" the protocol is at least on the order of 280 cryptographic operations. For on-line attacks impractical means that the number of possible on-line trials is very small compared to the number of possible key or password values.
Min-entropy	A measure of the difficulty that an attacker has to guess the most commonly chosen password used in a system. In this document, entropy is stated in bits. When a password has n-bits of min-entropy then an attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The attacker is assumed to know the most commonly used password(s).
Network	An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties. Unless otherwise stated no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking…) and passive (e.g., eavesdropping) attack at any point between the parties (claimant, verifier, CSP or relying party).
Nonce	A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.
Off-line Attack	An attack where the attacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing.
On-line Attack	An attack against an authentication protocol where the attacker either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets.
Passive Attack	An attack against an authentication protocol where the attacker intercepts data traveling along the network between the claimant and verifier, but does not alter the data (i.e. eavesdropping).
Password	A secret that a claimant memorizes and uses to verify ownership of his or her electronic digital credential. Passwords are typically character strings and must be protected from interception and be sufficiently difficult to guess. See also PIN.
Personal Identification Number (PIN)	A password consisting only of decimal digits.

Possession of a token	The ability to activate and use the token in an authentication protocol.
Proof of Possession (PoP) protocol	A protocol where a claimant proves to a verifier that he or she possesses and and can make use of a token (e.g., a private key or password).
Public Key Certificate	A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. See also [RFC 3280].
Registration	The process through which a party applies to become a subscriber of a IdP and an RA validates the identity of that party on behalf of the IdP.
Registration Authority	A trusted entity that establishes and vouches for the identity of a subscriber to a IdP. The RA may be an integral part of a IdP, or it may be independent of a IdP, but it has a relationship to the IdP(s).
Relying Party	An entity that relies upon an assertion offered by another party. An IdP relies on an assertion from a claimant offering a credential. A service provider relies on an IdP to offer a correct assertion of identity on behalf of that Subject, typically to process a transaction or grant access to information or a system.
Repudiation	Intentional denial of being a registrant (i.e., identity Subject claims that he/she did not register that token) or of authentication (i.e., identity Subject intentionally compromises his/her token, to repudiate authentication).
Service Provider	A relying party that offers access to on-line information, resources or other services based on some aspect of the identity of users.
Session Cookie	Small transient file that contains information about an end user that disappears when the end user's browser is closed. Unlike a persistent cookie, a transient cookie is not stored on an end user's hard drive, but is only stored in temporary memory that is erased when the browser is closed.
Shared Secret	A secret used in authentication that is known to the claimant and the verifier. There are two durations for a shared secret: • Session (temporary) secret – duration of the secret is limited to the duration of the user session. That is, the secret is created, used, and expired during a single user authentication session. • Long-term secret - duration of the secret persists ongoing, and is used from one user authentication session to another user authentication session.
Subject	The person or other entity whose identifier is bound in a particular credential. A party who receives a credential or token from an IdP and becomes a claimant in an authentication protocol.
Subscriber	A party who applies for a digital credential or token from an IdP operator on behalf of itself or another entity.
Token	A physical device that contains an electronic identity credential, cryptographic key, or dynamically derived bit string used to verify a claimant's association with an identity known to the IdP.
Tunneled	A protocol where a password is sent through a protected channel. For

Password Protocol	example, the TLS protocol is often used with a verifier's public key certificate to (1) authenticate the verifier to the claimant, (2) establish an encrypted session between the verifier and claimant, and (3) transmit the claimant's password to the verifier. The encrypted TLS session protects the claimant's password from eavesdroppers. See [RFC 5246]
Verifier	An entity that verifies the claimant's credential by verifying the claimant's possession of the associated token or authentication secret using an authentication protocol. As part of this, the verifier also may need to verify status of the credential.
Zero Knowledge password	A password such that Claimant does not tell receiver anything about the password the receiver does not already know.

Appendix B: Acronyms

Acronym	Definition
ANSI	American National Standards Institute
ASC	Authentication Service Component
ATO	Authorization To Operate
CISA	Certified Information Systems Auditor
COOP	Continuity of Operations Plan
CSP	Credential Service Provider
DR	Disaster Recovery
FIPS	(U.S.) Federal Information Processing Standard
HMAC	Hash-based Message Authentication Code
IAAF	Identity Assurance Assessment Framework
IAP	Identity Assurance Profile
IAQ	Identity Assurance Qualifier
ID	Identification
IdMS	Identity Management System
IdP	Identity Provider
ISO	International Organization for Standardization
IT	Information Technology
IVP	Identity Verification Process
NIST	National Institute of Standards and technology
OMB	Office Of Management And Budget (Federal government)
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comment (see www.ietf.org)
RP	Relying Party
SAML	Security Assertion Markup Language
SP	Service Provider
SSL	Secure Socket Layer
TLS	Transport Layer Security

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 "Credential Assessment Framework" Release 2.0.0.

Editors

David Wasley	Peter Alterman	John Krienke
Karl Heins	RL "Bob" Morgan	Steven Carmody
Tom Barton	David Walker	

Status	Release	Date	Comment	Audience
Draft			First release	Limited
				Public

Note: 29 Oct 2008 -- added eavesdropper; added phrase about change to IAPs in intro to section 2.