Identity Assurance Assessment Framework

April 16, 2012

Version 1.2

Release Candidate (Draft 5)

EXECUTIVE SUMMARY

The degree to which a Service Provider is willing to accept an Assertion of Identity from an Identity Provider may depend on how the Identity Provider Operator registers Subjects, issues Credentials, and manages the Identity information associated with Credentials. A set of requirements for these and possibly other aspects of Subject Identity that may be needed by Service Providers becomes an Identity Assurance Profile. Identity Provider Operators that meet the requirements of an Identity Assurance Profile can be certified as such by InCommon after passing a thorough assessment by a qualified independent party. Service Providers may choose to accept only Assertions of Identity that are offered by certified Identity Providers and include a particular Identity Assurance Qualifier.

This InCommon Identity Assurance Assessment Framework document describes the Identity assurance trust model that InCommon has adopted including a functional model for Identity Provider Operators and a certification model describing how certification is accomplished. It categorizes different aspects of Identity Credential and Subject information management and the methodology that must be used in performing an assessment of an Identity Provider Operator.

The functional model upon which the assurance framework is based is described and important terms are defined in section 2 of this document.

The structure of an InCommon Identity Assurance Profile is discussed in section 3.

Section 4 of this document describes the process by which Identity Provider Operators become certified by InCommon as compliant with any Identity Assurance Profile. It describes the assessment and audit process and the specific qualifications auditors must have in order to perform such assessments.

The assessment process results in an audit report to the Identity Provider Operator and a summary of findings report delivered to InCommon. InCommon then determines whether one or more Identity Assurance Qualifiers can be used by the Identity Provider Operator. Upon approval by InCommon, the Identity Provider may then include the appropriate Identity Assurance Qualifier(s) as part of its Assertions of Identity.

This document could be used by a Service Provider or any other relying party that wishes to understand the rationale for trustworthiness of the binding between an Identity Subject and his or her authentication Credentials or other information in Assertions of Identity it might receive that are specifically addressed by an Identity Assurance Profile. An InCommon Service Provider may choose to make use of the presence or absence of specific Identity Assurance Qualifier(s) in deciding whether to rely on Assertions of Identity it receives.

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 Identity Assurance Profiles (IAPs) in order to further achieve this efficiency through structured requirements for trusted Identity intended to help mitigate risk for relying parties. This document defines the overall model and concepts upon which InCommon's Identity Assurance program is based. Other documents define the specific requirements for particular profiles.

There are at least three parties to any federated Identity transaction: the Identity Subject who uses an Identity Credential, the Identity Provider Operator who issues Credentials and maintains associated Identity information (see section 2 below), and the SP operator that uses Assertions of Identity to manage access to its services. 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 and the Subject by minimizing the likelihood that another person would be able to claim a Subject's Identity. The Subject and the IdP Operator trust the SP to use and protect appropriately Identity information it receives.

Assertions of Identity offered by certified InCommon Federation Identity Providers may be relied upon across a wide range of Service Providers because the InCommon Federation verifies adherence to community standards for Identity management and Assertion as described in this Identity Assurance Assessment Framework (IAAF).

The general structure of IAPs is described and processes involved in certifying an InCommon Federation IdP Operator are defined. Assertions of Identity must be supported 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 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 a defined framework for trustworthiness of a Subject's Identity.

The degree to which an IdP Operator meets or exceeds requirements in these areas will determine which of the IAPs that IdP Operator is capable of supporting. Qualified IdP Operators can include the corresponding Identity Assurance Qualifier (IAQ) in Assertions of Identity that their IdP makes to SPs. SP operators that require assurance that an IdP can offer sufficiently trustworthy Assertions should understand this IAAF and accompanying profiles and then determine which InCommon IdP Operators have been certified as eligible to include the required IAQ. The SPs then can check that the Assertions received actually contain the required IAQ.

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

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

It is strongly recommended that SP operators use an industry accepted risk assessment methodology to assess potential risks associated with access to their online resources and then confirm that an IdP's certified IAQ(s) indicate conformance with an Identity assurance profile sufficient for the particular application. **The SP is solely responsible for determining whether a given profile is sufficient to mitigate any risks it might face as a result of relying upon Assertions conforming to that profile.**

The specific criteria used to assess IdP Operators are grouped into Identity Assurance Profiles, the structure of which is described in Section 3. Nothing in sections 1-3 of this document is normative. **Normative criteria to be used in an assessment process are expressed in separate Identity Assurance Profile documents**.

In order for an IdP Operator to be certified as compliant with an InCommon defined Identity Assurance Profile, the processes described in section 4 are mandatory unless specifically stated otherwise in an IAP.

From time to time it may become necessary or appropriate for InCommon to modify this IAAF or any IAP. IdPOs must come into conformance with relevant new or modified requirements within a reasonable period of time as determined by InCommon.

The InCommon Federation Identity Assurance document suite is available on the InCommon website at http://www.incommon.org/assurance/

1.1 RELATED DOCUMENTS

The reader should be familiar with the InCommon Federation Operating Policies and Practices [InC-FOPP] and the InCommon Federation Participation Agreement [InC-FPA]. Identity Assurance Profile documents [InC-IAP] refer to terms defined in this document.

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 Provider Operators that may offer Assertions of Identity to Federal agency applications. The InCommon Federation has adopted compatible terminology, guidance and requirements.

OMB M-04-04 defines the required level of Identity assurance in terms of the likely consequences of an Identity error. As the consequences of an Identity error become more serious, the required level of assurance increases. The OMB guidance provides Service Providers with example 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.

NIST Special Publication 800-63-1provides 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, Credentials, system hardware, authentication protocols and related Assertions.

The federal government Identity, Credential, and Access Management (ICAM) program has articulated requirements for IdPs that wish to interoperate with Federal agency applications. These requirements, documented in the Trust Framework Provider Adoption

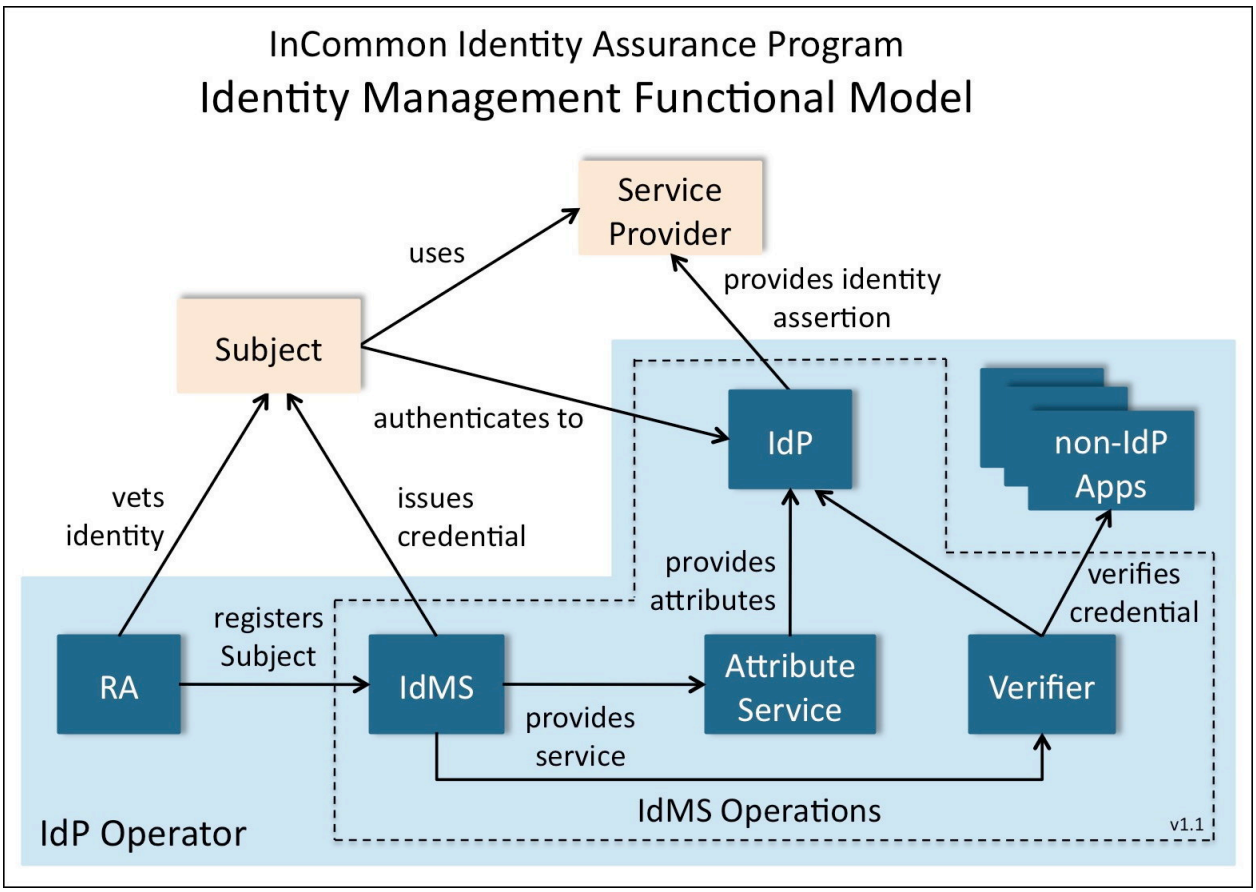
159 Process (TFPAP), are based on the above documents but also include requirements for
160 privacy and protection of Subject information and for qualification of auditors assessing an
161 IdP Operator. [F-ICAM]

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

164

2 IDENTITY MANAGEMENT FUNCTIONAL MODEL

This section presents a model for the components involved in the Identity management (IdM) practice of an organization operating an Identity Provider (IdP). Identity Assurance Profiles (IAPs) state requirements for the operation of these components. This IdM model is not the only way to organize the functions of an Identity management system, but serves as a reference for the description of assurance requirements, and to identify which components are in scope for such requirements.



Identity, as used in InCommon documents, refers to the set of information that pertains to a Subject. This includes identifiers, memberships, eligibility, roles, names, characteristics, etc. In an Assertion of Identity, these elements are referred to as *Attributes* or *Identity Attributes*.

The organization operating an IdP is an *IdP Operator* (IdPO). The term IdP Operator refers to the legal entity that signs contracts, is a registered participant in InCommon, and is responsible for the overall processes supporting the IdP. Thus, for example, for a university IdP it is the university that is the IdPO, not the internal organization that provides the service. It is the IdPO that is responsible for the service operating in compliance with an IAP regardless of how or where they are implemented, including outsourced or delegated arrangements.

The IdPO is responsible for ensuring IAP conformance by the elements in the shaded area in the diagram above. The elements within the dashed boundary constitute Identity

Management System Operations which includes the IdMS itself and related components.

The *IdP* is the system component that issues Assertions on behalf of Subjects (also known as users) who use them to access the services of *Service Providers* (SPs) (also known as *Relying Parties* or RPs). *Assertions* (sometimes called Identity Assertions) are structured data objects containing information about Subjects and other data useful for authentication and access, and are digitally signed by the issuer (the IdP). These Assertions are validated and consumed by SPs and the information in them is used by SPs for access control, personalization, and other purposes. The IdP also may include an *Attribute Service* that provides Subject Attributes in response to queries from SPs.

To do its job, the IdP relies on a number of other system components, such as Credential verifiers and Subject registration processes. If the IdPO is an organization offering only IdP services, these components are likely to be dedicated solely to supporting the IdMS operation. In an enterprise setting, the IdP is typically only one component in a set of Identity management services that support many enterprise functions. For example, a password verifier used by the IdP may also be used by other enterprise systems that need to verify passwords. Since this enterprise scenario is typical of InCommon participant organizations, and it is more complex than the dedicated-IdP scenario, this model focuses on the enterprise scenario.

A *Subject* is a person who is (or will be) registered with the IdPO, and has obtained (or will obtain) a Credential for use with the IdP. *Registration* is the process of creating a record of the Subject's identifying information. Registration typically includes Identity proofing, which is a process that involves checking the validity of Identity documents and ensuring that they apply to the Subject. In the enterprise setting, registration is sometimes done as part of general business processes such as hiring of employees and enrollment of students, in which case registration records are maintained in business systems, e.g., Human Resources (HR) and Student Information System (SIS), supporting these functions. Registration is performed by a *Registration Authority* (RA). In an enterprise there may be many RAs with many different registration processes.

An *Address of Record* for the Subject provides a means of contacting the Subject. The Address of Record could be a postal mail address, an e-mail address, a telephone number (fixed or mobile) or similar mechanism by which the Subject can receive communications from the IdPO.

Enterprise Identity and access management needs typically are met by a set of functions called an *Identity Management System* (IdMS). An IdMS includes a database of Subjects (an *IdMS database*) with information about people and other entities gathered from other enterprise databases such as HR and SIS. The IdMS database stores identifiers for Subjects, some provided by source systems and others created, managed and provided by the IdMS.

The IdMS database also stores Credentials for Subjects. A *Credential* is a unique identifier and associated authentication material used by the Subject to authenticate to the IdP. A UserID/password pair is the most common form of Credential; a public-key certificate and associated private key is another form. A Credential also may be issued to a Subject on a hardware device, e.g., a smartcard. A Subject may have more than one Credential bound to his or her record in an IdMS. Each Credential is associated with exactly one Subject

record.

The term *Authentication Secret* is used generically for passwords, passphrases, PINs, symmetric keys and other forms of secrets used for authentication. An Authentication Secret may also be generated by a *Token*, which is a physical device (or specialized software on a device such as a mobile phone) used in authentication. Authentication Secrets are vulnerable to guessing attacks, so resistance to guessing is an important IAP requirement. Requirements for protection of Secrets in transit and storage also may be needed.

Credential issuance is a key step in enabling Subjects to authenticate securely. Credential issuance may happen as part of the registration process, or may happen separately. Issuance involves creating the Credential such that it is bound to the Subject's IdMS record, and such that the Authentication Secret (or other authentication material) is available to the Subject and only to the Subject. As with registration, in an enterprise there are likely to be many Credential issuance processes.

As part of the authentication process, the IdP often uses a *Verifier* to validate the correctness of offered authentication material, for example a userID and password. Often this Verifier also serves applications other than the IdP. As such the characteristics of those other systems and their use of the Verifier may also be in scope for IAP requirements. A Verifier generally does its work via access to a *Credential Store* which contains Authentication Secrets for all Subjects. The Credential Store may be part of the IdMS database, or be provisioned from it. Proper protection of this store is particularly important in the overall security of the IdMS. In some enterprise scenarios the Credential Store, or a portion of it, is copied into different systems to support different authentication technologies or vendor platforms. In this case all Credential Store locations are likely to be subject to IAP requirements.

The Subject uses a *User Agent* (typically a web browser) to authenticate to the IdP and convey the Assertion to the SP. The authentication method used between the User Agent and the IdP, including protection of Authentication Secrets in transmission and storage, may be subject to IAP requirements. The protocol used between the IdP and the SP (via the User Agent) is also in scope for IAP requirements, as it should resist various attacks and support SP needs for assured Subject Identity.

Assertions sent by the IdP often contain more than one Identity Attribute relevant to the Subject (Identity Attributes may also be provided to SPs separately via an Attribute Service). The IdP may obtain these Identity Attributes directly from the IdMS database, from an attribute-specific service (such as an LDAP directory) provisioned from the IdMS, or from other sources. Since Identity Attributes may be used by SPs for security purposes the integrity of Attribute sources may be in scope for IAPs. InCommon recommends several defined Attributes for use by its participants.[3]

IdMS Operations refers to the technical environment and operating procedures supporting the IdMS. Since secure operation of the IdMS is critical to the effective assurance of the IdP, IAPs typically place constraints on technical measures and/or personnel used in IdMS Operations that may or may not apply to other enterprise systems.

[3] See http://www.incommon.org/attributesummary.html

The security of communications between system components (IdP, IdMS, Verifier, etc.) is important. A *Protected Channel* uses industry-standard cryptographic methods to provide integrity and confidentiality protection, resistance to replay and man-in-the-middle attacks, and mutual authentication. For example, SSL/TLS provides these protections.

A particular IdMS and IdP may support several different IAPs. They also may contain records and include processes that aren't in scope or don't meet the requirements of any IAP. As long as the factors related to a particular Subject (registration, issuance, authentication, etc.) meet the requirements of an IAP, Assertions about that Subject may include the IAQ for that IAP.

3 IDENTITY ASSURANCE PROFILES

An InCommon Identity Assurance Profile (IAP) specifies a set of criteria that, if met or exceeded by an IdPO, provide a useful metric by which an SP might determine whether Assertions of Identity conforming to those criteria can be used to help manage access to its service(s). InCommon defines IAPs in response to the well-articulated requirements of a community of interested SPs and IdPs. It is intended that the number of different profiles be minimized by making each one applicable to the broadest possible number of SPs.

Sufficient assurance of an Identity may involve many factors including registration of a Subject in an IdMS, 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 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.

InCommon IAPs are not necessarily hierarchical in nature. They represent particular sets of Identity management practices and requirements intended to address different use cases. An IdPO might support any number of IAPs and not all Subject records in a given IdMS need meet the requirements of all supported IAPs. In some cases, an IdPO conforming with a given IAP thereby also may conform with another, less stringent IAP and thus could apply for both certifications. An IdPO qualifying for InCommon Silver may be able to qualify readily for InCommon Bronze. An IdP may include in Assertions only those IAQs for which it has been certified and then only if all requirements for that IAQ have been met for the Subject of that Assertion.

InCommon IdP Operators are not required to qualify under any of the defined IAPs. InCommon IdP Operators are required only to self-describe their Identity management practices and make that statement available to InCommon SPs.[4] There is no InCommon Identity Assurance Qualifier (IAQ) for Assertions provided solely on the basis of this self-described profile.

It is a responsibility of the IdPO, as defined in the Identity Assurance Addendum to the InCommon Participation Agreement, to never knowingly include an IAQ in an Assertion that has not been assigned to it by InCommon and to ensure that any IAQ that is included is appropriate for the particular Subject Assertion being offered.

3.1 STRUCTURE OF INCOMMON IDENTITY ASSURANCE PROFILES

InCommon IAPs aggregate Identity assurance criteria into eight categories, each of which addresses related issues pertaining to an aspect of ensuring that an Assertion of Identity is valid and correctly associated with a given Subject. Criteria to address issues in each category are defined in each IAP if relevant. An IAP also might cover requirements on out-sourced or shared components of an IdPO's operations. If no criteria are needed in a category, the IAP will state that. Additional types of issues may be covered as needed.

3.1.1 BUSINESS, POLICY AND OPERATIONAL CRITERIA

An IAP might address the nature of the organization supporting the IdPO and its ability to

[4] InCommon Participant Operational Practices requirements: http://www.incommon.org/policies.html

provide a trustworthy and reliable IdP service. For example, it might be necessary for an IdPO to be a legal entity, or a function 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 might be required to demonstrate adequate resources and infrastructure to support the services it offers.

3.1.2 REGISTRATION AND IDENTITY PROOFING

Identity proofing is the process by which an IdPO or its designated Registration Authority (RA) or Registration Authorities associate a particular physical person with an existing Identity information record in the IdPO's IdMS database, or obtains and verifies the personal information required to create a new record for that physical person. Typically the Subject will be required to provide one or more authoritative documents or references from trusted sources of authority in order to ensure a reliable IdMS database record for that Subject. If the IdPO is a function of a larger organization, then Identity Subjects that are associated with that organization (e.g., employees and/or students) may have undergone some or all of the required Identity proofing during the process of bringing each person into the larger organization. It also might be possible to make a case for the comparability of long-term relationships where, for example, the organization has successful personnel experience with an employee over a number of years, financial information has been submitted successfully to the employee's bank or the IRS, etc.

During Identity proofing, sufficient information may be required to enable the IdPO to contact the Subject or, for some profiles, locate the Subject if necessary. An IAP might require that the Address of Record be verified, e.g., as part of Registration or Credential issuance. If a specific type of address is required in an IAP, e.g., residence or postal mail, this must be distinguished explicitly in the IAP.

Some profiles may require a record of the Identity proofing steps taken and/or authoritative documents presented by the Subject be retained as well, for example to show proof of process or to aid in re-establishing an Identity association at a future time.

3.1.3 CREDENTIAL TECHNOLOGY

A digital electronic Credential is the means by which an Identity Subject authenticates to an IdP Verifier. The "strength" of this Credential – its resistance to third party use, spoofing or discovering the Credential Authentication Secret – is a primary factor in determining the trustworthiness of the binding between a user of the Credential and the IdMS record for its Subject.

For shared secret Credentials, e.g., userID/password, the IAP might address how the Authentication Secret must be sufficiently difficult for a person other than the Subject to determine through trial and error, or other means and must be protected from illicit capture or replay. For physical token-based Credentials, the IAP might address how the Credential must be resistant to misuse if lost or stolen. The NIST document [SP 800-63] provides guidance on the strength of various digital electronic Credential technologies.

In some cases a given Subject may have more than one Credential to accommodate different authentication scenarios or a Subject might have several Credentials of different types. In this case the IAP might require that an IAQ in an Assertion be different depending on which Credential was used. Other factors might be significant such as

location of the Subject (e.g., on the campus network or on some remote network). Thus Assertions on behalf of each Subject might fall under different profiles depending on the type of Credential that was used and other factors. Similarly, if the IdPO is aware of a possible compromise of a Subject's Credential, an IAP might require that an Assertion contain a different IAQ or no IAQ, or that the IdPO suspend or invalidate the Credential for the purpose of Assertions until the concern is resolved.

Real-time re-authentication of the Subject by the IdP's Verifier might be required by some SPs if the current authentication event occurred too long in the past.[5] With some Credentials, e.g., smartcards, the IAP might require a built-in timeout in the Subject's device. If such re-authentication capability is required by an IAP, it may limit the types of Credentials that can be supported by the IdPO.

3.1.4 CREDENTIAL ISSUANCE AND MANAGEMENT

Creating and conveying a Credential to a Subject is a critical process that may be vulnerable in various ways. An IAP might define requirements to ensure that the Subject actually receives the Credential, has control of the Authentication Secret, and that no other person might acquire the Authentication Secret during the process. The IAP also might address Credential reissuance and/or revocation.

It is important to note that registration, Identity proofing, and Credential issuance represent different aspects of the same process. In many cases, however, this process may be broken up into a number of separate physical encounters and electronic transactions. An IAP might require that in these cases methods be used to ensure that the same party acts as Subject throughout the entire process.

3.1.5 AUTHENTICATION PROCESS

An authentication event occurs when a Subject offers his or her Credential to an IdP's Verifier. The Verifier interacts with the Subject to confirm he or she is the rightful physical person associated with the Credential and that the Credential is still valid. An IAP might define requirements to ensure this transaction is secure against interception or exposure of any Authentication Secret to any unauthorized party. The time, date, and nature of the authentication event may need to be recorded and the record retained for a reasonable period of time to aid in problem resolution or forensic analysis. Information about the most recent authentication event for a Subject, for example when it occurred, might be required as part of an Assertion.

Some SPs may wish to request reconfirmation of authentication where, in their judgment, the most recent event occurred too long in the past and they wish to confirm that the identified Subject is still in control of the current session. If this capability is required of the IdP, the IAP should address what constitutes sufficient reconfirmation.

3.1.6 IDENTITY INFORMATION MANAGEMENT

Assertions offered by the IdP to an SP will be based on information about or pertaining to the Subject, e.g., "name" or "unique identifier," obtained from reliable sources and held in an IdMS. Management of the IdMS database that stores this information is critical to the

[5] See also section 3.1.5.

degree of assurance that an Assertion might carry. An IAP might include requirements about the sources of Identity information, how it is obtained, and how information is maintained and updated when needed.

Identifiers generated for an IdPO's Subjects may be used by SPs to manage access. An IAP might address whether a given Subject may have any number of identifiers and whether a given identifier will map only to one specific Subject. IAPs may need to include requirements regarding the uniqueness or persistence of Subject identifiers, e.g., the length of time an assigned identifier is required to be bound to a given Subject or whether an identifier may be reassigned to a different Subject and, if so, whether there must be a period of time before reassignment.

Actions that affect the integrity or contents of the IdMS database may need to be logged securely and in a manner that is resistant to tampering. An IAP might place corresponding requirements on IdMS Operations, e.g., to aid in problem resolution or forensic analysis.

3.1.7 ASSERTION CONTENT

Assertions contain Identity information Attributes in structured, named information objects that refer to or pertain to the Identity Subject. Identity Attributes recommended for use by all InCommon IdPs and SPs are described on the InCommon Federation Attribute Summary [InC-AtSum].

An IAP might address what Attributes IdPs should convey to SPs and whether Subjects should be able to determine what Attributes, if any, will be conveyed to SPs. Real-time Subject consent processes may be used to control the release of personally identifiable information (PII) from the IdP to the SP. Alternatively, an IdPO might be required to obtain prior approval for release of certain PII.

IAPs might include provisions to address the required authoritativeness of some or all information conveyed in Assertions.

3.1.8 TECHNICAL ENVIRONMENT

An IAP may need to address security of the physical, technical and network environment and the adequacy of controls and procedures in place for all critical components of the IdPO's IdMS(s). All personnel with access to critical systems might be required to have Credentials as least as robust as the strongest Credentials that will be issued by those systems. To the extent possible, the IdPO's system architecture may need to be resistant to denial of service attacks.

An IAP might address how operating software on all service platforms involved in the IdP Operations, including registration, IdMS and Attribute Service databases, and Assertion processing, should be kept up to date and security-related software patches installed promptly.

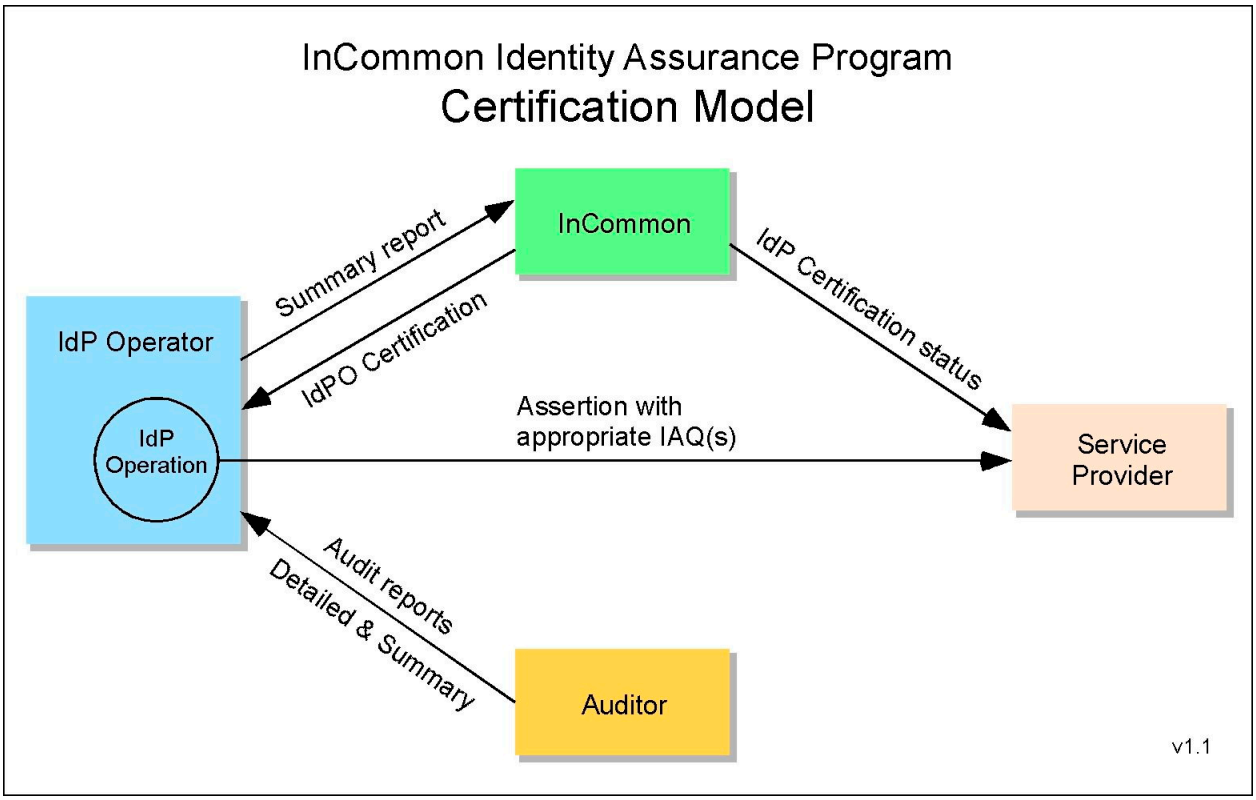
An IAP also might address how IdPOs should participate in problem resolution with SPs. It might be important to define requirements for reporting on and/or participating in response to breach of security or similar incidents.

An IAP might address how IdPOs provide for continuity of Identity verification and Assertion services in case of system failures or natural disasters. For example, by requiring

445 that system designs guard against erroneous Assertions or false positive authentication in
446 cases of partial system failure, minimizing single points of failure, providing backup or
447 stand-by service platforms, or replicating critical data to off-site locations.
448
449

4 ASSESSMENT AND AUDIT OF IDENTITY PROVIDERS

Unless otherwise specified in the relevant IAP, InCommon IdP Operators that wish to assert conformance to a specific InCommon IAP are required to undertake initial assessment and then arrange for an independent audit of that assessment, and, for some IAPs, periodic reassessment and audit of the controls for its IdMS Operations. InCommon does not perform such assessments or audits. The IdP Operator initiates the process and engages the Auditor. The Auditor reports to the IdPO and creates the summary report required by InCommon. The IdPO will convey the summary report to InCommon along with any other materials required by InCommon. InCommon makes the final determination regarding conformance.



The IdMS Operation must be fully operational and supported by the organization at the time of assessment. An IdPO may support several IdMS Operations but only those assessed and certified by InCommon may assert InCommon IAQs.

4.1 AUDITOR QUALIFICATIONS

The Auditor may be either an external contractor or may be a member of an internal audit office within the IdPO's organization. The Auditor doing the review must be objective and independent, following guidelines established by professional audit organizations such as The Institute of Internal Auditors "Standards for the Professional Practice of Internal Auditing".[6]

[6] http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/

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 IdPO's 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 IdPO's industry and services;
- General knowledge of the technologies/techniques being assessed;
- Technical and management audit experience;
- Familiarity with the applicable IAP(s); and
- Familiarity with this IAAF.

To audit an IdP Operator, the Auditor must have current direct experience as an information technology auditor and perform audits regularly in a professional capacity. Demonstrated qualification, such as designation as a Certified Information System Auditor[7] (CISA) or equivalent knowledge and experience, is required.

4.2 AUDIT PROCESS AND REPORT

The Auditor must conduct the audit in accordance with standards such as the Statements on Standards for Attestation Engagements developed by the American Institute of Certified Public Accountants[8]. The Auditor must prepare and sign a summary report including the auditor's opinion attesting to the IdPO's management assertions regarding compliance with the specific IAP(s). For a suggested report format example, see AICPA AT §601.58.

This summary report will be conveyed to the IdPO and must:

- State the date on which this audit was completed;
- Identify the Auditor, including qualifications;
- Outline the audit methodology; and
- State whether the IdPO conforms with all requirements of each IAP.

The IdPO provides this summary report to InCommon in its application for certification. If the IdPO used any alternative means to meet specific IAP requirements, it must also provide a document describing these means.

All audit summary reports and attachments will be kept in confidence by InCommon.

4.3 INCOMMON'S REVIEW AND ACTION

InCommon will review the Auditor's summary report and consider the impact of any alternatives noted in the IdP Operator's assessment. If the nature of the alternatives appear minor and would have little negative impact on the IdPO's Identity assurance, InCommon may choose to accept them. In some cases it may be necessary to work with the IdPO to understand the rationale for an alternative. If significant negative impact on the assurance of Identity in Assertions is found, InCommon will require the IdPO to correct them. When

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

[8] See AICPA's Statements on Standards for Attestation Engagements
http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx

corrected, the IdPO must have the Auditor review the correction and submit an updated summary report to the IdPO to be conveyed to InCommon.

4.4 IDENTITY PROVIDER CERTIFICATION

Once the audit results are accepted by InCommon, the IdP Operator is certified by InCommon to assert one or more IAQs. InCommon will place the IAQ(s) in the IdP metadata describing the IdP. SPs and other relying parties are expected to acquire this information as part of an InCommon participant metadata refresh cycle.

4.5 CONTINUING IDPO COMPLIANCE

Once the IdP Operator is certified by InCommon to be compliant with one or more IAPs, periodic reassessments may be required. If so, this will be specified in the relevant IAP(s). For some IAPs, self-reassessment or a declaration of changes to the IdP Operation may be sufficient. If a complete re-assessment is required, then the auditor qualifications and reporting requirements above apply.

4.5.1 CHANGES TO IDPO OPERATIONS

When changes to an IdPO's operation are reported, InCommon will determine whether the changes are sufficient to require reassessment. Any change-driven reassessment would only need to cover those elements that have changed.

4.5.2 SECURITY BREACH OR OTHER INCIDENTS

When security related breaches or other service related incidents that might impact compliance with an IAP are reported to InCommon, InCommon will work with the IdPO to determine an appropriate remediation of such incidents.

4.5.3 IDENTITY PROVIDER OPERATOR SUSPENSION OR DECERTIFICATION

If deficiencies in the IdP Operations are reported to InCommon by the IdPO, or reported by an affected party and confirmed by InCommon, InCommon will allow the IdPO a reasonable period of time to correct any such deficiencies. Failure of the IdPO to provide required reports is considered a deficiency in this context. The length of the grace period will depend on the severity of the deficiency with respect to its impact on the assurance of Assertions made by the IdP. If the deficiency is deemed by InCommon to have significant impact, the IdPO may be required to suspend the use of the IAQ in Assertions it makes and this will be reflected in metadata for the affected IdP. This suspension will be lifted upon receipt of a statement from the IdPO and satisfactory to InCommon that the deficiency has been corrected.

If the deficiencies are not corrected during the grace period, the IdPO's certification for use of the relevant IAQ may be revoked. Conditions for re-certification will be defined by InCommon on a case by case basis.

APPENDIX A: REFERENCES

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

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

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

[InC-FOPP] "**Federation Operating Policies and Practices**", InCommon Federation, http://www.incommon.org/policies.html

[InC-FPA] "**Participation Agreement**", InCommon Federation, http://www.incommon.org/policies.html

[InC-IAP] InCommon Federation Identity assurance profiles, http://www.incommon.org/assurance/

[F-ICAM] **Identity, Credential, and Access Management**, Federal government http://www.idmanagement.gov/

APPENDIX B: ACRONYMS

Acronym	Definition
CISA	Certified Information Systems Auditor
FOPP	Federation Operating Policies and Practices
HR	Human Resources
IAAF	Identity Assurance Assessment Framework
IAP	Identity Assurance Profile
IAQ	Identity Assurance Qualifier
ICAM	Identity, Credential, and Access Management
IdM	Identity Management
IdMS	Identity Management System
IdP	Identity Provider
IdPO	IdP Operator
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office Of Management And Budget (US Federal government)
PIN	Personal Identification Number
RA	Registration Authority
SIS	Student Information System
SP	Service Provider
TFPAP	Trust Framework Provider Adoption Process

APPENDIX C: DEFINED TERMS

Certain terms are defined in this document and must be used consistently in all Identity Assurance Profiles that reference this document. Full definitions are contained in the text of this document on the page indicated. Brief descriptions are listed here for convenience.

Defined Term	Page	Brief summary description
Address of Record	p5	A means of contacting the Subject.
Assertion	p5	Structured data objects containing Identity information and other relevant data. Sometimes called Identity Assertions.
Attributes	p4	Elements of an Identity.
Attribute Service	p5	Provides Subject Attributes in response to queries from SPs.
Authentication Secret	p6	Used generically for passwords, passphrases, PINs, symmetric keys and other forms of secrets used for authentication
Credential	p5	A unique identifier and authentication material.
Credential Store	p6	Contains Authentication Secrets for all Subjects
Identity	p4	Information that is true about a Subject.
Identity Attributes	p4	Information elements relevant to a Subject.
Identity Management System	p5	A set of functions serving the Identity and access management needs of an enterprise.
Identity Provider	p5	The IdMS system component that issues Assertions.
IdMS database	p5	A database of IdMS Subjects.
IdMS Operations	p6	The technical environment supporting the IdMS.
IdP Operator	p4	The organization operating an IdP is an *IdP Operator*.
Protected Channel	p7	A communication mechanism that provides message integrity and confidentiality protection.
Registration	p5	The process of creating a record of a Subject's Identity information.
Registration Authority	p5	A trusted entity entitled to perform Registrations.
Relying Parties	p5	A synonym for Service Provider.
Service Provider	p5	Uses an Identity Assertion as part of managing access to its services.
Subject	p5	A person who is (or will be) registered with the IdP Operator
Token	p6	A physical device (or specialized software on a device such as a mobile phone) used in authentication.
User Agent	p6	Typically a web browser, used by the Subject to authenticate to the IdP and convey the assertion to the SP.
Verifier	p6	Validates the correctness of offered authentication material.

APPENDIX D: DOCUMENT HISTORY

This document was developed by the InCommon Federation Technical Advisory Committee with significant contributions from other experts and reviewers.
http://www.incommon.org/about.html

EDITORS

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

Status	Release	Date	Comment	Audience
Public	1.0	4 Nov 2008	First full release for implementation	Open
Draft	1.0.2	24 Mar 2010	Revisions to align with ICAM TFPAP	Open
Public	1.0.3	22 Apr 2010	Added to Glossary "FIPS" under "Approved"	Open
Draft	1.0.4	10 Jun 2010	Modified 3.1 to satisfy ICAM	Open
Draft	1.1D1	18 Dec 2010	Greatly modified to remove unnecessary elements and clarify remaining elements	Limited
Draft	1.1D4	21 Jan 2011	Further significant mods based on IdP Functional Model	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 for consistency, etc.	Limited
Draft	1.1FD2	15 Apr 2011	Final revisions prior to SC review	Limited
FINAL	1.1	9 May 2011	Approved by InCommon Steering Committee	Public
Draft	1.2v4	10 April 2012	Clarified audit section; added information about conformance to new IAAF and IAP versions. Approved for community review by Assurance Advisory Committee	Limited
Public	1.2RC (Draft 5)	16 April 2012	Release Candidate Available for Public Comment	Public