InCommon Bronze Self-Certification
September 26, 2014

This document contains the compliance assertions of Harvard University regarding InCommon Assurance Profile 1.2.

Name of organization: Harvard University
Name of contact: Scott Bradner
Email address: scott_bradner@harvard.edu
Date: September 26, 2014

Specification of Identity Assurance Requirements

This section contains all of the normative language for the Bronze and Silver IAPs. In the requirements that follow, *(B)* indicates that the numbered section applies to the Bronze IAP; *(S)* indicates that the section applies to the Silver IAP.

0.0 Background

Harvard assigns a University identification number (HUID) to most members of the Harvard Community. HUIDs are assigned to individuals "for life," and care is taken to ensure that each individual is assigned only a single HUID and that multiple individuals are not assigned the same HUID. HUIDs are not sequentially assigned, but do have some structure to assignation, so are not completely random. HUIDs are not considered public information.

For many years, Harvard has had a home-built central authentication system known as the PIN system. In 2013, a CAS-based authentication system was implemented and a shim layer was developed to mimic the old PIN system in order to preserve the user interface and to continue to support existing applications. The database that the CAS system uses includes all currently active HUID holders and many of the people who were assigned HUIDs but who are no longer active, as well as holders of a few other types of identifiers.

In addition, Harvard has a central University Active Directory system that includes all currently active HUID holders.

Some individual Harvard Schools maintain their own local authentication systems.

The University Shibboleth IdP uses CAS as its authentication engine. CAS can authenticate users directly, by making use of the University Active Directory, or by using the Harvard Medical School's local authentication system. The University Shibboleth IdP will only assert HUID holders, and only those HUID holders that have been authenticated by an authentication system self-certified as compliant with the InCommon Bronze requirements to InCommon Bronze service providers (SPs). This document covers the University CAS and Active Directory authentication systems.

Hundreds of existing applications currently use the PIN/CAS system, and the use of Active Directory is widespread. Most new applications use native CAS, the University Shibboleth IdP, or Active Directory for authentication.

Currently both the PIN/CAS system and the University Active Directory use their own credential management systems, but credential management for both the CAS and Active Directory systems is being moved to a common identity management system. New users will be able to claim accounts and existing users will be able to perform identity-management self-service — including password management — though this system. New or updated identity and authentication credentials will then be pushed both to CAS and to Active Directory when changes are seen. Because credentials will be common between the IdP, PIN/CAS, and Active Directory, both PIN/CAS and Active Directory need to be considered in-scope for this assurance.

Harvard has not had, and does not currently have, a University-level password expiration requirement; the University community has resisted adding such a requirement. Thus, many current passwords may not meet current password strength requirements. To compensate for this, the University IdP will check the timestamp of the last password change to ensure it was after the password change mechanism that enforces the current standards was installed. This will ensure that individuals being authenticated for InCommon SPs are using passwords with the proper strength.

The University authentication systems and identity management system are managed by Harvard University Information Technology (HUIT), a central administration group that manages University-wide services and provides IT services and support for most of the Harvard Schools.

1.0 Business, Policy, and Operational Criteria

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

1.1 (S, B) InCommon Participant

The IdPO must be an InCommon Participant in good standing in order to be considered for certification under this IAP.

Harvard has been an InCommon member in good standing since April 2012.

Harvard's Participant Operational Practices are posted at http://iam.harvard.edu/resources/incommon-participant-operational-practices.

1.2 (S, B) Notification to InCommon

The IdP Operator must notify InCommon of any circumstance that may affect the status of its compliance with this IAP.

1. The IdP Operator must notify InCommon of any significant changes to its operation that may affect the status of its compliance and hence its qualification under this IAP. Notification should occur no less than 30 days before the changes are to be made effective, or as soon as practicable after an unanticipated change is noted.

Harvard will notify InCommon of any significant changes in our operation that might affect the status of our compliance with this set of assurance requirements.

2. The IdPO must report to InCommon any breach of security or integrity of its IdMS Operations that may affect the status of its compliance and hence its qualification under this IAP. A report must be made as soon as practicable after any such incident is noted.

Harvard will provide timely notification to InCommon of any breach in security or integrity of our IdMS operations that might affect the status of our compliance with this set of assurance requirements.

1.3 (S, B) Continuing Compliance

After initial certification by InCommon, IdP Operators must declare to InCommon continued compliance with profiles under this IAP at least every 3 years.

Harvard will declare its compliance with the then-current set of InCommon assurance requirements at least every three years.

1.4 (S, B) IDPO Risk Management

The IdPO's Information Technology operations must align with the organization's risk management objectives as demonstrated by a periodic review process or other equivalent control.

University Risk Management and Audit Services (RMAS) meets annually with HUIT management to review HUIT's alignment with University policies and goals.

2.0 Registration and Identity Proofing

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

2.1 (S) RA Authentication

Each RA must authenticate to the IdMS using a credential that meets or exceeds Silver requirements.

This requirement does not apply to InCommon Bronze-level certification, but login access — including by RAs to the systems, including CAS servers, Active Directory servers, IdDB database servers, and LDAP servers, that support IMS operations — requires the use of a multi-factor, encrypted VPN tunnel in addition to individual account credentials (which must meet the same length and complexity requirements as do normal user credentials).

Communications between an RA and the IdMS shall be encrypted using an Approved Algorithm that also authenticates the IdMS platform.

This requirement does not apply to InCommon Bronze-level certification, but see section 2.1 for further details.

2.2 (S) **Identity Verification Process**

1. *The identity proofing and registration process shall be performed according to written policy or practice statements that specify the particular steps taken by IdPO staff or systems to verify identities.*

This requirement does not apply to InCommon Bronze-level certification, but Harvard has produced policies and procedures that cover identity proofing for the population that the Harvard IdP will assert to any InCommon Bronze or Silver SP. Harvard has adopted written procedures for identity proofing when picking up ID cards, and U.S. federal processes apply when hiring new paid employees. In addition, Harvard is developing written procedures for in-person identity proofing when the proofing is done as a separate function.

2. *The above statement(s) shall address the primary objectives of registration and identity proofing, including:*
   - *Ensuring a person with the claimed identity information does exist, and that the identity information is sufficient to uniquely identify a single person within the IdPO's range of foreseeable potential Subjects;*
   - *Ensuring that the physical person requesting registration is entitled to the claimed identity.*

This requirement does not apply to InCommon Bronze-level certification, but Harvard follows the in-person proofing requirements described in section 2.4.2 and the existing relationship requirements described in section 2.4.1 to ensure that the person being registered exists and that registration is being done by that person.

2.3 (S) **Registration Records**

1. *A record of the facts of registration shall be maintained by the IdPO.*

This requirement does not apply to InCommon Bronze-level certification, but records about all user registrations are maintained in the Harvard IdMS database (known as the IdDB).

2. *The record of the facts of registration shall include:*
   - *Identity proofing document types and issuers;*
   - *Full name as shown on the documents;*
   - *Date of birth;*
   - *Current Address of Record.*

This requirement does not apply to InCommon Bronze-level certification, but Harvard meets these requirements for the population that the University would assert to an InCommon Bronze or Silver SP. That population includes paid employees as well as those HUID holders who have picked up a physical HUID card or who have undergone an in-person identification verification process during which they provided a government-issued photo ID.

The central University identity database (known as IdDB) maintains a considerable amount of information about individuals who have been assigned HUIDs. Relevant to this document, said information includes full legal name, birthdate, a partial SSN or other national ID (when available), current postal address, the type of document used to prove identity, and, when proofing has been explicitly done, the date that proofing was performed and who performed the proofing. Relevant information from this database is published via two LDAP servers. CAS uses one of these LDAP servers to store and verify user credentials, and both servers to obtain user attributes. These two LDAP servers are currently being merged into a single server. The identification issuer is not recorded at this time, but changes to capture this information are underway.

3. *Records also must include revocation or termination of registration.*

This requirement does not apply to InCommon Bronze-level certification, but the status fields in IdDB records are used to indicate revocation or termination.

4. *Registration records must be retained for 7.5 years beyond the expiration of any credential issued to the Subject by the IdPO.*

This requirement does not apply to InCommon Bronze-level certification, but records are kept in the Harvard IdDB indefinitely.

2.4 (S) **Identity Proofing**

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

2.4.1 **Existing Relationship**

If the IdPO is a function of an enterprise, the identity proofing process may be able to leverage a pre-existing relationship, e.g., the Subject is an employee or student. Where some or all of the identity proofing done at the time the existing relationship was established is comparable to that required in §2.4.2 or §2.4.3 below, those results may be relied upon for this purpose. The IdPO's Registration Authority (RA) shall confirm that the Subject is a person with a current relationship to the organization, record the nature of that relationship and verify that the relationship is in good standing with the organization.

This requirement does not apply to InCommon Bronze-level certification, but — as mentioned above — the individuals Harvard asserts to an InCommon Bronze or Silver SP are HUID holders who are paid employees as well as HUID holders who have picked up a physical HUID card or have otherwise undergone a special in-person identification verification where they presented a government-issued photo ID as part of the process. Paid employees are considered to have been identity-proofed due to their existing relationship to the University. Recently-hired paid employees have undergone the identity checks that have been required by federal regulation for many years. Employees who were hired before current Harvard identity verification regulations went into effect are considered identity-proofed because the University, by virtue of filing multiple years' worth of tax information on these individuals and sending W-2 forms to postal addresses of record, can be certain that these addresses are correct. The University would have been notified in the event of filing tax information on the wrong person or on a non-existent individual. We specifically do not include non-paid employees in the "existing relationship" category, since these employees do not undergo the same level of identity verification.

Information about what type of ID was used for identity proofing is captured for people who pick up ID cards and will be captured for people who undergo a special in-person identity proofing process (see section 2.3.2). Information about what type of ID was used for identity proofing is not available for paid employees who have not picked up an ID card, or those who did not present a government issued-ID when they did pick up an ID card. Individuals, other than paid employees, who do not have an ID type recorded in IdDB will not be asserted by the Harvard IdP to an InCommon Silver SP. The ID issuer is not currently captured, but changes to capture this information are underway.

2.4.2 **In-Person Proofing**

1. *The RA shall establish the Subject's IdMS registration identity based on possession of a valid current government photo ID that contains the Subject's picture (e.g., driver's license or passport), and either an address or nationality.*

Harvard will also assert those HUID holders who have picked up a physical ID card and who have presented a government-issued photo ID as part of the pickup process.

2. *The RA inspects the photo ID and compares the image to the physical Subject. The RA records the document type and issuer, the address given on the ID if there is one, and the date of birth shown on the ID if there is one. If the ID appears valid, the photo matches the physical Subject, and the ID confirms the Subject's date of birth, the RA authorizes issuance of Credentials.*

The card pickup process records the type of identification provided, verifies that the name, photo, and date of birth shown on

the identification are the same as information existing in the identity database, and verifies that the photo on record, the ID, and the person picking up the ID card all match. Individuals are instructed to go though a formal process to update the database information if the data in the IdMS database does not match that on the offered ID. The ID issuer is not currently captured, but changes to capture this information are underway.

Harvard does occasionally issue ID cards for which the process described above is not followed, but the database records of those individuals do not indicate that identity was verified and, thus, are not asserted by the Harvard IdP to an InCommon Bronze or Silver SP unless they are a paid employee.

In the future, Harvard also will have a separate in-person identity verification process that will operate in the same manner as the ID card pickup process.

3. *If the address given on the ID does not confirm the Address of Record, the Address of Record must be confirmed as described in §2.5 below.*

This requirement does not apply to InCommon Bronze-level certification, but the electronic address of record is verified during the account claiming or password change processes. The Harvard processes do not generally verify postal address of record.

2.4.3 **Remote Proofing**

1. *The RA shall establish the Subject's IdMS registration identity based on possession of at least one valid government ID number (e.g., a driver's license or passport) and either a second government ID number or financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number.*

Harvard does not support remote proofing at this time. Individuals who do not have the proper existing relationship, have not picked up a ID card, or who have not undergone a special identity verification process will not be asserted to an InCommon Silver SP.

2. *The RA verifies other information provided by the Subject using both of the ID numbers above through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, date of birth, and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. If this appears to be the case, the RA authorizes issuance of Credentials.*

Not applicable — see 2.4.3.1.

3. *If the record checks do not confirm the Address of Record, it must be confirmed as described in §2.5 below.*

Not applicable — see 2.4.3.1.

2.5 (S) **Address of Record Confirmation**

The Address of Record must be confirmed before the Subject's record can be considered to meet the requirements of this IAP. If the Address of Record was not confirmed as part of Identity proofing, then it must be accomplished by one of the following methods:

1. *The RA contacts the Subject at the Address of Record and receives a reply from the Subject; or*

This requirement does not apply to InCommon Bronze-level certification, but the account claiming process for new University account holders and the credential change processes for existing account holders involves an exchange of email to an address of record.

2. *The RA issues Credentials in a manner that confirms the Address of Record supplied by the Subject.*
    a. *For a physical Address of Record, the RA requires the Subject to enter online a temporary Secret from a notice mailed to the Subject's Address of Record.*

Harvard does not verify a physical address of record other than for a paid employee or during a specific type of credential reset. Postal addresses of record are verified for paid employees by sending W-2 forms only to such addresses. In the case of one type of password reset, a letter including an alphanumeric token is sent via postal mail to the physical address of record

and the user enters this token into a web page. If Harvard needed to do business with an InCommon SP requiring a verified physical address, Harvard would configure the IdP to only assert HUID holders who have undergone the paper-mail-based credential reset, or would establish a special verification process for physical addresses of record for HUID holders that needed to use that SP. Harvard will institute a mechanism to verify paper addresses of record if this becomes an issue.

b. *For an electronic Address of Record, the RA confirms the ability of the Subject to receive telephone communications at a telephone number or e-mail at an e-mail address. Any Secret not sent over a Protected Channel shall be invalidated upon first use.*

This requirement does not apply to InCommon Bronze-level certification, but the account claiming process for new University account holders involves an exchange of email to an address of record. By default, this process also captures and verifies a telephone number to be used as a second factor in a credential (e.g., password) change process. The token used in this process is invalidated when it is first used or after 24 hours, whichever is earlier.

2.6 (S, B) **Protection of Personally Identifiable Information**

Any personally identifiable information collected during registration or identity proofing must be protected from unauthorized disclosure or modification.

The University identity database is considered to include high-risk information, and is thus inaccessible from the Internet or open parts of the Harvard network. Access is further restricted to those applications and individuals that have a business requirement for specific information from the database. Account and individual access is restricted to the specific records and fields for which there is a proven business requirement.

3.0 **Credential Technology**

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

3.1 (S, B) **Credential Unique Identifier**

1. *Each Credential issued by the IdPO shall include a unique identifier (e.g., userID, Distinguished Name, serial number) that distinguishes it from all other Credentials in use by the IdPO.*

Harvard uses the HUID to uniquely identify individuals. Additional identifiers are assigned to some members of the Harvard Community, but the Harvard IdP will only make InCommon Bronze assertions for individuals who have been assigned HUIDs.

2. *A Subject can have more than one Credential unique identifier, but a given Credential unique identifier must map to at most one Subject.*

Care is taken to ensure that the HUID identifies only one individual and that an individual does not have multiple HUIDs.

3. *The IdPO shall clearly associate the Credential unique identifier to the Subject's registration record in the IdMS, for use by the Verifier or other parties.*

The HUID is a unique key used in the University identity database.

3.2 (B) **Basic Resistance to Guessing Authentication Secret**

The Authentication Secret and the controls used to limit online guessing attacks shall ensure that an attack targeted against a given Subject's Authentication Secret shall have a probability of success of less than 2-10 (1 chance in 1,024) over the life of the Authentication Secret. This requires that an Authentication Secret be of sufficient complexity and, in most cases, that the number of invalid attempts to enter an Authentication Secret for a Subject be limited.

Refer to NIST Special Publication 800-63-1 [SP 800-63], Appendix A, for a discussion of Authentication Secret complexity and resistance to online guessing.

Harvard's common identity management system enforces the use of complex passwords of at least 10 characters in length. The password character set includes uppercase and lowercase alphabetic, numeric, and the suite of special characters. The complexity requirement is for at least one uppercase, one lowercase, and one non-alphabetic character in each password. Candidate passwords are also checked against a large dictionary and against directory information about the individual. Both CAS and Active Directory lock a user out for at least 30 minutes after 10 bad password guesses. The University does not require regular password changes, but the University IdP will ensure that passwords used to authenticate individuals for InCommon Bronze SPs have been changed within the last five years, in essence enforcing a five-year password reset requirement that impacts only users of InCommon Bronze SPs. With these conditions, Harvard meets Bronze requirements for basic resistance to guessing. See the appendix for calculations showing the level of guessing resistance.

3.3 (S) **Strong Resistance to Guessing Authentication Secret**

1. *The Authentication Secret and the controls used to limit online guessing attacks shall ensure that an attack targeted against a given Subject's Authentication Secret shall have a probability of success of less than 2-14 (1 chance in 16,384) over the life of the Authentication Secret. This requires that an Authentication Secret be of sufficient complexity and that the number of invalid attempts to enter an Authentication Secret for a Subject be limited.*

See the discussion under section 3.2. In addition, the University IdP will ensure that any password used to authenticate an individual to an InCommon Silver SP has been changed within the last year, in essence enforcing a one-year password reset requirement impacting only users of InCommon Silver SPs. With these conditions, Harvard meets Silver requirements for basic resistance to guessing. See the appendix for calculations showing the level of guessing resistance.

2. *The Authentication Secret shall have at least 10 bits of min-entropy to protect against an untargeted attack. Refer to NIST Special Publication 800-63-1 [SP 800-63], Appendix A, for a discussion of Authentication Secret complexity and resistance to online guessing and how to calculate min-entropy.*

This requirement does not apply to InCommon Bronze-level certification, but the password requirements described in section 3.2 provide at least 10 bits of min-entropy based on Appendix A.2.2 of NIST 800-63-2. The password setting and change system checks candidate passwords against a dictionary of more than 2 million words, as well as directory information about the user in order to ensure that permutations of personal information, including username, are not used.

3.4 (S) **Stored Authentication Secrets**

Authentication Secrets shall not be stored as plaintext. Access to encrypted stored Secrets and to decrypted copies shall be protected by discretionary access controls that limit access to administrators and applications that require access.

Three alternative methods may be used to protect the stored Secret:

1. *Authentication Secrets may be concatenated to a variable salt (variable across a group of Authentication Secrets that are stored together) and then hashed with an Approved Algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen Authentication Secret file are not useful to attack other similar Authentication Secret files. The hashed Authentication Secrets are then stored in the Authentication Secret file. The variable salt may be composed using a global salt (common to a group of Authentication Secrets) and the userID (unique per Authentication Secret) or some other technique to ensure uniqueness of the salt within the group of Authentication Secrets; or*

This requirement does not apply to InCommon Bronze-level certification, but the University does not currently meet this requirement with either CAS or Active Directory password storage. Both currently use unsalted hashes for storing passwords. Salted hashes will be implemented for CAS in late 2014, with the salted hash captured the first time a user successfully logs in after the function goes live.

2. *Store Secrets in encrypted form using Approved Algorithms and decrypt the needed Secret only when immediately required for authentication; or*

This requirement does not apply to InCommon Bronze-level certification; however, the University currently meets this requirement for CAS but not for Active Directory. Whole-disk encryption has been enabled for CAS, and will be maintained at least until the salted hash function is enabled. Active Directory does not support the use of salted hashes, so whole-disk encryption will be implemented on the Active Directory servers before Harvard will authenticate for InCommon Silver SPs.

3. *Any method protecting stored Secrets at NIST [SP 800-63] Level 3 or 4 may be used.*

Not applicable.

3.5 (B) Basic Protection of Authentication Secrets

1. *Authentication Secrets shall not be stored as plaintext. Access to stored Secrets and to plaintext copies shall be protected by discretionary access controls that limit access to administrators and applications that require access.*

Passwords are stored in a hashed form in the CAS server password storage and the Active Directory servers. See section 3.4.2 for further details. Access to the stored passwords is limited to the proper small set of administrators using access controls that meet the requirements of section 5.

2. *Plaintext passwords or Secrets shall not be transmitted across a network.*

All interactions between users and the CAS and Active Directory servers use HTTPS. Temporary secrets sent to the email or postal address of record are not encrypted.

3.6 (S) Strong Protection of Authentication Secrets

1. *Any Credential Store containing Authentication Secrets used by the IdP (or the IdP's Verifier) is subject to the operational constraints in §3.4 and §8 (that is, the same constraints as IdMS Operations). When Authentication Secrets are sent from one Credential Store to another Credential Store (for example in an account provisioning operation) Protected Channels must be used.*

This requirement does not apply to InCommon Bronze-level certification, but encrypted channels are used by the common credential management system and the credential stores used by the PIN/CAS system and by Active Directory. AD will be configured to use AES before Harvard qualifies for InCommon Silver. Because all domain controllers run Windows 2008 or higher and are properly configured, synchronization of passwords between domain controllers is protected by AES encryption, which is an Approved Algorithm. Provisioning activities to the Active Directory Domain Controller all take place over LDAPS, which uses an Approved Algorithm.

2. *Whenever Authentication Secrets used by the IdP (or the IdP's Verifier) are sent between services for verification purposes (for example, an IdP to a Verifier, or some non-IdP application to a Verifier), Protected Channels should be used, but Protected Channels without client authentication may be used.*

This requirement does not apply to InCommon Bronze-level certification, but LDAPS is required for all access to the LDAP server that includes the credential store. AD will be configured to use LDAPS and disable all domain support of the LM and NTLMv1 protocols before Harvard will qualify for InCommon Silver.

3. *If Authentication Secrets used by the IdP (or the IdP's Verifier) are exposed in a transient fashion to non-IdP applications (for example, when users sign on to those applications using these Credentials), the IdPO must have appropriate policies and procedures in place to minimize risk from this exposure.*

This requirement does not apply to InCommon Bronze-level certification, but in the few cases where a system other than PIN/CAS or Active Directory (e.g. the network access control system) captures passwords, the systems that capture user credentials are covered by detailed security requirements.

4.0 Credential Issuance and Management

The authentication Credential must be bound to the physical Subject and to the IdMS record pertaining to that Subject.

The account claiming process binds a physical subject to the IdMS record.

4.1 (S, B) Credential Issuance

To ensure that the same Subject acts throughout the registration and Credential issuance process, the Subject shall identify

himself or herself in any new transaction (beyond the first transaction or encounter) with information known only to the Subject, for example a temporary Secret which was established during a prior transaction or encounter, or sent to the Subject's Address of Record. When identifying himself or herself in person, the Subject shall do so either by using a Secret as described above, or through the use of an equivalent process that was established during a prior encounter.

The account claiming process for new University account holders involves an exchange of email to an address of record. The claiming process requires the individual enter a temporary secret token sent to the address of record as part of the process. The token is disabled after 24 hours or after it is used, whichever is first.

The account claiming process is the first part of the credential setting process, during which the user sets his or her password. The password is known only to the user and is not stored in any readable or reversible format. The password established during the account claiming process is used in subsequent authentications.

4.2 (S, B) **Credential Revocation or Expiration**

1. *The IdPO shall revoke Credentials within 72 hours after being notified that a Credential is no longer valid or is compromised.*

Credential validity is based on status fields in the central University identity database. These status fields are changed when an individual's status changes. The IdMS group can receive requests from the Office of General Counsel, the HR office, or the University security office to invalidate existing passwords under defined and documented circumstances. The IdMS group immediately resets the password and, in cases where it is required, modifies the IdDB to block the user from establishing a new password.

2. *If the IdPO issues Credentials that expire automatically within 72 hours or less then the IdPO is not required to provide an explicit mechanism to revoke the Credentials.*

Electronic temporary credentials expire after 24 hours unless used before then, in which case they expire when first used. Printed temporary credentials expire when first used.

4.3 (S, B) **Credential Renewal or Re-Issuance**

A Subject must be authenticated for purpose of Credential renewal or re-issuance by any of the following methods:

A common credential management system is used to manage credentials. The answers below refer to this system.

1. *By use of a non-expired and valid Credential.*

Credential (password) changes can be made in the common identity management system after a user is authenticated using their existing credential (password) if he or she knows it.

2. *By use of a single-use secret delivered to the Subject from the IdPO by means of a pre-registered out of band delivery mechanism.*

The credential reset process involves sending a single-use token to the email address of record or, in the future, either by sending a single-use token to or interacting with an app on a portable device registered during the initial account claiming process.

3. *The Subject may supply correct answers to pre-registered personalized questions designed to be difficult for any other person to know. After expiration of the current Credential, if none of these methods is successful then the Subject must re-establish her or his identity with the IdPO per Section 2 before the Credential may be renewed or re-issued. Authentication Secrets shall not be recovered; new Authentication Secrets shall be issued.*

A question-based authentication mechanism will not be supported in the new credential reset process.

4.4 (S) **Credential Issuance Records Retention**

The IdPO shall maintain a record of the unique identifier and time of issuance or revocation of each Credential issued or revoked for a minimum of 7.5 years beyond the expiration of the Credential.

This requirement does not apply to InCommon Bronze-level certification, but this information is kept indefinitely in the IdMS.

4.5 (S, B) **Resist Token Issuance Tampering Threat**

The process or processes used by the IdPO in 4.1, 4.2, and 4.3 must enable the Subject to verify that the IdPO is the source of any token or Credential data they receive.

The user will only receive a token after they have requested one, so an unsolicited token must be false. In addition, the user must interact via HTTPS with a web server to initiate the token sending, the web server that uses a certificate to validate its identity.

5.0 **Authentication Process**

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

Users authenticate using known-only-to-them passwords. For multi-factor, users must also take an action to acknowledge a challenge sent to a pre-registered portable device or enter a token sent to such a device.

5.1 (S, B) **Resist Replay Attack**

The authentication process must ensure that it is impractical to achieve successful authentication by recording and replaying a previous authentication message.

The mechanisms used by the PIN, CAS, and Active Directory systems use timestamps and hidden tokens to limit the possibility of a replay attack. In addition, the authentication event resists replay attack by forcing the user to enter authentication credentials separately to the IdP — rather than capturing the credentials elsewhere and forwarding them to the IdP — and using protected channels for this communication.

5.2 (S, B) **Resist Eavesdropper Attack**

The authentication protocol must resist an eavesdropper attack. Any eavesdropper who records all the messages passing between a Subject and a Verifier or relying party must find that it is impractical to learn the Authentication Secret or to otherwise obtain information that would allow the eavesdropper to impersonate the Subject.

All authentication communications between PIN/CAS and Harvard IdP users and servers are encrypted using HTTPS or LDAPS to prevent eavesdropping.

For Active Directory, all requirements for this section are handled via the same mechanisms as defined for section 3.6.2: The authentication event resists replay attack by forcing the user to enter authentication credentials separately to the IdP — rather than capturing the credentials elsewhere and forwarding them to the IdP — and using protected channels for this communication.

5.3 (S, B) **Secure Communication**

Communication between Subject and IdP must use a Protected Channel.

All communications between the user's browser and the Harvard IdP are over HTTPS.

5.4 (S, B) **Proof of Possession**

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

The user is required to provide a known-only-to-the-user password as part of the authentication process for both PIN/CAS and Active Directory authentication. The Harvard IdP uses the Harvard CAS system as its authentication engine. A multi-factor mechanism will soon be deployed and will employ a device registered as being in the possession of the user during his or her account claim process. This multi-factor function will be used in the password reset process, as well as being required for specific systems or individuals.

5.5 (S, B) **Resist Session Hacking Threat**

Session maintenance methods implemented by the IdP shall resist session hijacking.

The Shibboleth IdP employs SSL encryption, along with a secure cookie management strategy, for session maintenance and to limit session hijacking.

5.6 (S, B) **Mitigate Risk of Credential Compromise**

The IdPO must have policies, practices, or guidelines in place that prohibit Subjects from sharing their Credentials and mitigate risks of a Subject's Credential being acquired by someone else through other means. Subjects must be informed of these policies, practices or guidelines and educated about the importance of keeping their Credentials secure.

The University enterprise information security policy prohibits sharing user credentials. All users are informed of these requirements.

6.0 **Identity Information Management**

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

6.1 (S, B) **Identity Record Qualification**

If Subject records in an IdMS do not all meet the same set(s) of IAP criteria, then the IdP must have a reliable mechanism for determining which IAQ(s), if any, are associated with each record.

As discussed in a number of locations above, the Harvard IdP checks information in the LDAP servers to determine what level of assurance, if any, can be asserted for an individual.

7.0 **Assertion Content**

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

The Harvard IdP takes its attribute information from an LDAP server that is a reflection of the information in the Harvard IdMS, the authoritative source of attribute information.

7.1 (S, B) **Identity Attributes**

The actual meaning of any attribute values identified as attributes recommended for use by InCommon Participants should be consistent with definitions in the InCommon Attribute Summary [InC-AtSum].

The attributes that the Harvard IdP provides conform to InCommon attribute definitions. The attributes that are provided are configured on a per-SP basis from a list that includes *eduPersonScopedAffiliation, eduPersonPrincipalName, sn, givenName, displayName, eduPersonUniqueID,* and *mail*.

7.2 (S, B) **Identity Assertion Qualifier (IAQ)**

An IdPO may be certified by InCommon to be eligible to include one or more InCommon IAQs as part of Assertions. The IdP ***must not*** *include an InCommon IAQ that it has not been certified by InCommon to assert and* ***must not*** *include an IAQ if that Assertion does not meet the criteria for that IAP. The IdP must be capable of including an InCommon IAQ when the necessary criteria are met for the Subject.*

As discussed in a number of locations above, the Harvard IdP checks information in the LDAP servers to determine what level of assurance, if any, can be asserted for an individual.

7.3 (S, B) **Cryptographic Security**

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

The Assertion must be either:

- *Digitally signed by the IdP; or*

The Harvard IdP uses standard InCommon Shibboleth software. The IdP will be reconfigured such that SAML assertions sent to any InCommon SP after January 15, 2015 requesting an InCommon Assurance Profile will be signed using a SHA 2 algorithm.

- *Obtained by the SP directly from the trusted entity (e.g., the IdP or Attribute Service) using a Protected Channel.*

Harvard does not support the SAML *AttributeQuery* function for fetching attributes from the IdP.

8.0 Technical Environment

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

8.1 (S) Software Maintenance

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

This requirement does not apply to InCommon Bronze-level certification, but all systems that support IdMS operations make use of standard software systems (e.g. CAS and Active Directory) and are included in a standard patch schedule.

8.2 (S) Network Security

1. *Appropriate measures shall be used to protect the confidentiality and integrity of network communications supporting IdMS operations. Protected Channels should be used for communications between systems.*

This requirement does not apply to InCommon Bronze-level certification, but login access to the systems that support IMS operations — including the CAS servers, Active Directory servers, IdDB database servers, and LDAP servers — is protected by both network-level and host-based firewalls and access control filters.

2. *All personnel with login access to IdMS Operations infrastructure elements must use access Credentials at least as strong as the strongest Credential issued by the IdPO*.

This requirement does not apply to InCommon Bronze-level certification, but login access to the systems that support IMS operations — including the CAS servers, Active Directory servers, IdDB database servers, and LDAP servers — requires the use of a multi-factor VPN tunnel in addition to individual account credentials that must meet the same length and complexity requirements as do normal user credentials.

8.3 (S) Physical Security

IdMS Operations shall employ physical access control mechanisms to restrict access to sensitive areas, including areas such as leased space in remote data centers, to authorized personnel.

This requirement does not apply to InCommon Bronze-level certification, but both the physical and virtual servers that are used to implement authentication services are located in University-owned and -operated secure data centers, secure hosting centers, or secure virtual environments. Physical access is restricted to the University data center and the hosting centers.

8.4 (S) Reliable Operations

IdMS Operations shall employ techniques to minimize system failures and ensure that any failures are not likely to result in inaccurate Assertions being sent to SPs.

This requirement does not apply to InCommon Bronze-level certification, but a fault-tolerant architecture is used for all IAM services. There are redundant servers for IdP, CAS, and PIN, and there are four redundant LDAP servers to support CAS and the IdP. All of these servers auto-failover in case of failure. The University Active Directory service includes six auto-failover servers. All systems are programmed in a way to minimize the chance that a false assertion could be sent to an SP.

9.0 US Federal ICAM Privacy Assurance

An InCommon Participant that configures its IdP to facilitate access to federal government agency applications must affirm that its practices are consistent with the requirements privacy criteria defined by the Federal Identity, Credentialing, and Access Management (FICAM) program in its TrustFramework Provider Adoption Process (TFPAP).

9.1 Written Notice of Attribute Release

Personnel and students who are required to make use of the IdP to connect with a federal agency application for business or educational purposes are given written notice, prior to the first use of the IdP for that purpose, regarding the federal agency application and identity information that will be transmitted to it. Written notice may be in paper or electronic form. The IdP will use an approved U.S. Federal government profile when interacting with Federal agency web sites.

Harvard has published a description of the personally identifiable information that is provided to InCommon SPs that use the Harvard IdP for authentication, as well as a list of the specific attributes provided to individual SPs (including the information provided to U.S. federal government SPs).

9.2 Participation in the IdP Service

Participation in the IdP service is incorporated as part of accepting enrollment in the institution's academic or research programs or entering into an employment contract.

All normal faculty, staff, and students are enabled for and expected to make use of the core authentication system used by the Harvard IdP.

9.3 Identity Provider Service Description

IdP Subjects are provided with a general description of the IdP service and how it operates. The service description also defines what personal information is collected, how it is managed and how errors or other concerns may be resolved.

Harvard has posted information on the core authentication system and IdP to the University's Identity and Access Management program website, located at iam.harvard.edu. This information includes how the systems work, what information is collected, who has access to the information and under what circumstances, how the systems are managed, and what users can do if they find errors or have other problems.

9.4 Information Provided to Federal Agency Applications

Information will be made available to a federal agency application only if there is prior agreement between the institution and the federal agency regarding what that information will comprise. Such information will be the least required. Whenever possible, an abstract identifier unique to the Subject will be used instead of personally identifying information (PII). The IdP will transmit only the information that is required by the federal application.

Harvard enables attributes for SPs that make use of its IdP on a per-SP basis — with the exception of *eduPersonPrincipalName* (EPPN), which is enabled by default. Harvard does not provide information other than via these attributes, and does not provide attributes that the SP does not require for proper operation.

9.5 Protection of Personal Data

PII recorded for Subjects is protected in storage and transmission as required by the InCommon IAP. IdP transaction data is collected and used strictly for problem resolution such as determining why a particular identity assertion was not successful or responding to a misuse of IdP privileges.

IdP transaction data is never made available to third parties except as might be required by law or regulation or as required for problem resolution by authorized individuals. IdP log files and databases are secured against unauthorized access and information that is no longer needed is destroyed.

The storage and transmission of PII gathered by the Harvard IdP during the authentication process meets the requirements of the InCommon IAP, and is used only for problem resolution or as part of an investigation (conducted in accordance with legal requirements or University policies) of possible misuse of privileges obtained through the use of the IdP.

Log files are properly protected against access or modification, and are discarded after 90 days.

9.6 **Problem Resolution**

Should an identity Subject or a relying party have concerns about whether the IdP is in compliance with the above or with any aspect of the IdP service as defined, the institution has established procedures for resolution of such concerns.

Harvard has published that anyone with concerns on the operation or details of compliance with InCommon requirements should email directory_services@harvard.edu.