InCommon Assurance Profile Management
Bronze Assertions

The following page contains the management assertions from the University of Nebraska Medical Center (UNMC) Identity Management Steering Committee regarding the InCommon Assurance Profiles, version 1.2.

4.2.1 Business, Policy, & Operational Criteria

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

Management Assertion

Our institution is a legal entity that is an InCommon Participant in good standing, and has the organizational structures and processes to comply with the provisions of this IAP.

4.2.1.1 InCommon Participant

The IdPO must be an InCommon Participant in good standing in order to be considered for certification under this IAP. In this context, “good standing” means not in arrears with respect to financial obligations to InCommon nor out of compliance with other contractual obligations to InCommon.

On September 14, 2012 University of Nebraska Medical Center received a copy of the completed InCommon Participant Agreement, signed by Deb Thomas of University of Nebraska Medical Center and John Krienke, InCommon CEO. The most recent membership payment of $1,600 was made on 11/29/12, as documented with payment receipt 11623. The University of Nebraska Medical Center is in compliance with other contractual obligations to InCommon, including posting our InCommon Participant Operational Practices.

4.2.1.2 Notification to InCommon

The IdP Operator must notify InCommon of any circumstance that may affect the status of its compliance with this IAP.
1. The IdP Operator must notify InCommon of any significant changes to its operation that may affect the status of its compliance and hence its qualification under this IAP. Notification should occur no less than 30 days before the changes are to be made effective, or as soon as practicable after an unanticipated change is noted.
2. The IdPO must report to InCommon any breach of security or integrity of its IdMS Operations that may affect the status of its compliance and hence its qualification under this IAP. A report must be made as soon as practicable after any such incident is noted.

1. The InCommon Administrative Contact for the University of Nebraska Medical Center will notify InCommon of any circumstance that may affect the status of University of Nebraska Medical Center's compliance with this IAP no less than 30 days before the changes are to be made effective, or as soon as practicable after an unanticipated changed is noticed.
2. The InCommon Administrative Contact for University of Nebraska Medical Center will report to InCommon any breach of security or integrity of its IdMS Operations that may affect the status of its compliance and qualification under this IAP. The report will be made as soon as practicable after any such incident is noted.

4.2.1.3. Continuing Compliance

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

4.2.1.4. 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.

A risk assessment is performed by the Information Security Officer in accordance with the Risk Assessment Procedure.

Evidence of compliance for audit

- Participation Fee Documentation
- Link to University of Nebraska Medical Center InCommon Participant Operational Practices
- Link to InCommon Participant Agreement
- Names of University of Nebraska Medical Center's InCommon Administrative and Executive Contacts:
  - InCommon Executive Contact – Yvette Holly
  - InCommon Federation Site Administrators – Lee Trant, Sharon Welna
- University of Nebraska Medical Center's Information Technology organization chart and organizational web pages:
  - Information Technology Services Organization Chart
  - About Information Technology Services
  - University of Nebraska Medical Center Risk Management Process Procedure
4.2.2 Registration & Identity Proofing

Note: 4.2.2.1 through 4.2.2.5 are not applicable for Bronze certification

4.2.2.6 Protection of Personally Identifiable Information

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

UNMC has an information security program based upon the NIST framework. The information security plan identifies the controls which are in place to protect the personally identifiable information. The organization utilizes information security industry best practices to define the development and implementation of the information security program. The program is based upon the National Information Security Standards (NIST) standards in conjunction with the SANS 20 critical security controls.

The organization recognizes that it has both internal and external risks. Under the direction of the Information Security Officer (ISO), the organization periodically performs a formal risk assessment of the environment. Based upon this risk assessment, a risk management process is implemented. As new major systems are implemented, a risk assessment of the system is performed and results integrated with the organization’s overall risk assessment.

All personally identifiable information (PII) collected during registration and proofing is protected from unauthorized disclosure and modification. The PII is data collected from the SAP and PeopleSoft system which are managed by the University of Nebraska Central System. Appropriate manual controls are in place to verify the data which is maintained in the systems.

Evidence of compliance for audit

- Information Security Plan
4.2.3 Credential Technology

Management assertions related to the credential technology used at the University of Nebraska Medical Center.

4.2.3.1 Credential Unique Identifier

1. Each Credential issued by the IdPO shall include a unique identifier (e.g., userID, Distinguished Name, serial number) that distinguishes it from all other Credentials in use by the IdPO.
2. A Subject can have more than one Credential unique identifier, but a given Credential unique identifier must map to at most one Subject.
3. The IdPO shall clearly associate the Credential unique identifier to the Subject’s registration record in the IdMS, for use by the Verifier or other parties.

NOTE: When an individual requests a name change and identifier change, it is possible that the InCommon entity will need to establish a new relationship with the individual.

4.2.3.2 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.

Password complexity is comprised of the following variables:

- 94 character set, plus complexity rules
  - Microsoft complexity rule setting
- Lockout duration of 40 hours
- Attempts before lockout 8
- Password length 8
- Password expiration 180 days

Per the University of Wisconsin-Madison Entropenator (Tests Against NIST 800-63), these parameters meet the Level of Assurance $2^{-10}$ (1 chance in 1,024).
4.2.3.4 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
2. Store Secrets in encrypted form using Approved Algorithms and decrypt the needed Secret only when immediately required for authentication; or
3. Any method protecting stored Secrets at NIST [SP 800-63] Level 3 or 4 may be used.

LDAP passwords are normally stored in the userPassword attribute. RFC4519 specifies that passwords are not stored in encrypted (or hashed) form. This allows a wide range of password-based authentication mechanisms, such as DIGEST-MD5 to be used. This is also the most interoperable storage scheme.

However, it may be desirable to store a hash of password instead. slapd(8) supports a variety of storage schemes for the administrator to choose from.

---

Note: Values of password attributes, regardless of storage scheme used, should be protected as if they were clear text. Hashed passwords are subject to dictionary attacks and brute-force attacks.

---

The userPassword attribute is allowed to have more than one value, and it is possible for each value to be stored in a different form. During authentication, slapd will iterate through the values until it finds one that matches the offered password or until it runs out of values to inspect. The storage scheme is stored as a prefix on the value, so a hashed password using the Salted SHA1 (SSHA) scheme looks like:

userPassword: {SSHA}DkMTwBl+a/3DQTxCYEApdUtNXGgdUac3

The advantage of hashed passwords is that an attacker which discovers the hash does not have direct access to the actual password. Unfortunately, as dictionary and brute force attacks are generally quite easy for attackers to successfully mount, this advantage is marginal at best (this is why all modern UNIX systems use shadow password files).
The disadvantages of hashed storage is that they are non-standard, may cause interoperability problem, and generally preclude the use of stronger than Simple (or SASL/PLAIN) password-based authentication mechanisms such as DIGEST-MD5.

**SSHA password storage scheme**

This is the salted version of the SHA scheme. It is believed to be the most secure password storage scheme supported by *slapd*.

These values represent the same password:

\[
\text{userPassword: } \{\text{SSHA}\}DkMTwB1+a/3DQTxCYEApdUtNXGgdUac3 \\
\text{userPassword: } \{\text{SSHA}\}d0Q0626PSH9VUld7yWpR0k6BlpQmtczb
\]

Campus AD DS stores passwords on a user object in the `unicodePwd` attribute. Windows generates and stores user account passwords by using two different hashes. When you set or change the password for a user account to a password that contains fewer than 15 characters, Windows generates both a LAN Manager hash (LM hash) and a Windows NT hash (NT hash) of the password. These hashes are stored in the local Security Accounts Manager (SAM) database or in Active Directory.

*Note: 4.2.3.5 is not applicable for Bronze certification*

**Evidence of compliance for audit**

- Entropy calculator document
4.2.4 Credential Issuance and Management

4.2.4.1 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 subject will identify him/herself using information only known to the subject.

4.2.4.2 Credential Revocation.

1. The IdPO shall revoke Credentials within 72 hours after being notified that a Credential is no longer valid or is compromised.
2. If the IdPO issues Credentials that expire automatically within 72 hours or less then the IdPO is not required to provide an explicit mechanism to revoke the Credentials.
We will revoke Credentials within 72 hours after being notified that a Credential is no longer valid or is compromised

4.2.4.3 Credential Renewal or Re-issuance

A Subject must be authenticated for purpose of Credential renewal or re-issuance by any of the following methods:
1. By use of a non-expired and valid Credential.
2. By use of a single-use secret delivered to the Subject from the IdPO by means of a pre-registered out of band delivery mechanism.
3. The Subject may supply correct answers to pre-registered personalized questions designed to be difficult for any other person to know.
After expiration of the current Credential, if none of these methods is successful then the Subject must re-establish her or his identity with the IdPO per Section 4.2.2 before the Credential may be renewed or re-issued. Authentication Secrets shall not be recovered; new Authentication Secrets shall be issued.

Passwords can be reset by the individual by accessing https://net.unmc.edu/netid/index.php/, supplying their login name and answers regarding personal information OR by Help Desk staff after the subject has provided personal information only known by the subject using the process defined in 4.2.4.1.

Note: 4.2.3.4 is not applicable for Bronze certification

4.2.4.5 Resist Token Issuance Tampering Threat

The process or processes used by the IdPO in 4.2.4.1, 4.2.4.2, and 4.2.4.3 must enable the Subject to verify that the IdPO is the source of any token or Credential data they receive.

The subject should access the campus network enter their account credentials consisting of user id and password which is comprised of components of personally identifiable information.

Evidence of compliance for audit

Life cycle Management Directory Server Accounts

Special Circumstances Separation Process

Information Security Incident Response Procedure

4.2.5 Authentication Process
4.2.5.1 - Resist Replay Attack

The Shibboleth authentication system includes countermeasures to resist replay attacks. Cookies and time-based authenticators are used to prevent replay attacks, also the tickets issued are stored to insure one-time-use are not valid after they have been verified.

4.2.5.2 - Resist Eavesdropper Attack

The Shibboleth and LDAP servers use secure communication between client and the LDAP login server. Binds to the LDAP server must use SSL/TLS for secure communication.

4.2.5.3 - Secure Communication

Communication between Subject and IdP must use a Protected Channel.

Management asserts that all communication between the Subject and the IdP is over a secure communication channel using https with AES 128bit encryption.

4.2.5.4 - Proof of Possession

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

When authenticating, the user enters their username and password which is only known to them.

4.2.5.5 - Session Authentication

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.

4.2.5.6 - 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.

Technical controls are in place to ensure that a strong password is created.
Evidence of compliance for audit

UNMC Metadata

*.unmc.edu
Issued by: Entrust Certification Authority – L1C
Expires: Saturday, March 26, 2016 1:31:57 AM Central Daylight Time
This certificate is valid

Details

<table>
<thead>
<tr>
<th>Subject Name</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>State/Province</td>
<td>Nebraska</td>
</tr>
<tr>
<td>Locality</td>
<td>Omaha</td>
</tr>
<tr>
<td>Organization</td>
<td>University of Nebraska Medical Center</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>ITS</td>
</tr>
<tr>
<td>Common Name</td>
<td>*.unmc.edu</td>
</tr>
</tbody>
</table>

| Issuer Name | US |
| Organization | Entrust, Inc. |
| Organizational Unit | www.entrust.net/rpa is incorporated by reference |
| Organizational Unit | (c) 2009 Entrust, Inc. |
| Common Name | Entrust Certification Authority – L1C |
| Serial Number | 1276907165 |
| Version | 3 |

Signature Algorithm: SHA–1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters: none

Not Valid After: Saturday, March 26, 2016 1:31:57 AM Central Daylight Time

Public Key Info

| Algorithm | RSA Encryption (1.2.840.113549.1.1.1) |
| Parameters | none |
| Public Key | 256 bytes: 81 25 ED 70 1A E9 3A D3 ... |
| Exponent | 65537 |
| Key Size | 2048 bits |
| Key Usage | Encrypt, Verify, Wrap, Derive |
| Signature | 256 bytes: 31 84 0F 53 C6 0C A1 38 ... |
Security in Shibboleth:

```xml
<!--
    Each attribute in these profiles configuration is set to its default value,
    that is, the values that would be in effect if those attributes were not present.
    We list them here so that people are aware of them (since they seem reluctant to
    read the documentation).
-->
<xp:ProfileConfiguration xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="http://www.w3.org/2001/XMLSchema-instance">
    <xp:IncludeAttributeStatement>`false`
        assertionLifetime="PT1M"
        signResponses="conditional"
        signAssertions="never"/>
    <xp:IncludeAttributeQueryProfile>`false`
        assertionLifetime="PT1M"
        signResponses="conditional"
        signAssertions="never"/>
    <xp:IncludeArtifactResolutionProfile>`false`
        assertionLifetime="PT1M"
        signResponses="conditional"
        signAssertions="never"/>
    <xp:IncludeAttributeStatement>`true`
        assertionLifetime="PT1M"
        signResponses="conditional"
        signAssertions="never"/>
    <xp:IncludeAttributeQueryProfile>`true`
        assertionLifetime="PT1M"
        signResponses="conditional"
        signAssertions="never"/>
    <xp:IncludeArtifactResolutionProfile>`true`
        assertionLifetime="PT1M"
        signResponses="conditional"
        signAssertions="never"/>
    <xp:IncludeAttributeStatement>`true`
        assertionLifetime="PT1M"
        signResponses="conditional"
        signAssertions="never"/>
    <xp:IncludeAttributeQueryProfile>`true`
        assertionLifetime="PT1M"
        signResponses="conditional"
        signAssertions="never"/>
    <xp:IncludeArtifactResolutionProfile>`true`
        assertionLifetime="PT1M"
        signResponses="conditional"
        signAssertions="never"/>
</xp:ProfileConfiguration>
```
<!-- Username/password login handler -->

<ph:LoginHandler xsi:type="ph:UsernamePassword"
    jaasConfigurationLocation="file:///opt/shibboleth-idp/conf/login.config">
    <ph:AuthenticationMethod xsi:type="SAML2.0" class="PasswordProtectedContent" ph:AuthMethod/>
</ph:LoginHandler>

<!-- DO NOT EDIT BELOW THIS POINT -->

<security:TrustEngine id="shibboleth.SignatureTrustEngine" xsi:type="security:SignatureChaining"/>
<security:TrustEngine id="shibboleth.SignatureMetadataExplicitKeyTrustEngine" xsi:type="security:MetadataExplicitKeySignature" metadataProviderRef="#security:SecurityPolicy"/>
<security:TrustEngine id="shibboleth.CredentialTrustEngine" xsi:type="security:Chaining"/>

<security:Rule xsi:type="samls2:Replay" required="false"/>
<security:Rule xsi:type="samls2:IssueInstant" required="false"/>
<security:Rule xsi:type="samls2:MandatoryIssuer"/>

<security:Rule xsi:type="samls2:Replay"/>
<security:Rule xsi:type="samls2:IssueInstant"/>
<security:Rule xsi:type="samls2:ProtocolWithXMLSignature" trustEngineRef="shibboleth.SignatureTrustEngine"/>
<security:Rule xsi:type="security:ClientCertAuth" trustEngineRef="shibboleth.CredentialTrustEngine"/>
<security:Rule xsi:type="samls2:MandatoryIssuer"/>
<security:Rule xsi:type="security:MandatoryMessageAuthentication"/>

<security:Rule xsi:type="samls2:Replay"/>
<security:Rule xsi:type="samls2:IssueInstant"/>
<security:Rule xsi:type="samls2:ProtocolWithXMLSignature" trustEngineRef="shibboleth.SignatureTrustEngine"/>
<security:Rule xsi:type="security:ClientCertAuth" trustEngineRef="shibboleth.CredentialTrustEngine"/>
<security:Rule xsi:type="samls2:MandatoryIssuer"/>
<security:Rule xsi:type="security:MandatoryMessageAuthentication"/>
4.2.6 Identity Record Qualifications

4.2.6.1 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.

Faculty, staff students and affiliates are stored in a unique OU within the Directory Server. Only this account within this OU may participate in federation. When a change occurs in student or employment status, a separation process is followed.

Evidence of compliance for audit

Life cycle Management Directory Server Accounts

Employee Separation

4.2.7 Assertion Content

4.2.7 Assertion Content

The IdPO (management) has 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.

See below for specific information about the documentation of IdPO practices which meet the requirements for each sub-section.

4.2.7.1 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]

Our institution supports the following list of eduPerson and other inetOrgPerson attributes as defined in the InCommon Attribute Summary:

- eduPersonPrincipalName
- eduPersonScopedAffiliation
- givenName
- sn
- mail

Our business populates the attributes based upon the data contained in the authoritative source of the Human Resource System (SAP), the Student Information System (People Soft) and affiliate accounts. Our business
rules populate the attributes in alignment with the eduPerson and inetOrgPerson object classes, which are linked from the InCommon attribute summary page:

http://www.incommonfederation.org/attributesummary.html

**4.2.7.2 Identity Assertion Qualifier**

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

We have not been qualified by InCommon to assert any identity qualifiers (IAQs) as of the time of writing of this documentation, and we currently do not release any IAQs for any Subjects.

We will store our IAQs as attribute values in the LDAP and Grouper data stores, but they are currently not populated nor accessible from the IdP.

We will not release any IAQ we have not been certified to release, in the future, using the same method.

**4.2.7.3 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
- Obtained by the SP directly from the trusted entity (e.g., the IdP or Attribute Service) using a Protected Channel.

The assertion content is protected via use of a TLS channel between the IdP and the SP for both the artifact resolution/attribute service port 8443 and the SSO (port 443) endpoints.

We do not list any non-TLS protected endpoints in InCommon metadata, and our IdP does not respond to requests in the clear.

The certificate used by our IdP for signing and encryption of assertion content is listed in InCommon metadata, and we can sign and encrypt assertion content on request.

The InCommon metadata ([http://wayf.incommonfederation.org/InCommon/InCommon-metadata.xml](http://wayf.incommonfederation.org/InCommon/InCommon-metadata.xml)) lists the endpoints of our IdP. Additionally, the IdP's relying-party.xml file lists configured endpoints for sets of entityIDs.

Use of OpenSSL to query and verify the certificates used on ports (443, 8443, etc.) of our IdP is possible.

**Evidence of compliance for audit**

We use x509, with the certificate in InCommon’s public metadata file and the key only possessed by UNMC:
From our login.config file

```xml
<security:Credential id="IdPCredential" xsi:type="security:X509Filesystem">
  <security:PrivateKey/>
  <security:Certificate/>
</security:Credential>
```

bindDN and bindCredential removed for security’s sake

```
mail="test"
userFilter=~uid={01}*z
```

## 4.2.8 Technical Environment

**Note:** 4.2.8 does not apply for bronze certification