The University of Texas System Identity Management Federation

Membership Operating Practices
September 1, 2006

Last Revised: 16 November, 2015

INTRODUCTION

The U.T. System Identity Management Federation (the "Federation") provides an integrated identity and access management infrastructure for The University of Texas System's ("U. T. System's") various institutions. This infrastructure enables individuals officially affiliated with and identified by a U. T. System institution that is a member of the Federation (a "Member") to use their institutionally certified digital credential(s) to access, when appropriate, restricted services provided by any other Federation Member. Federation Members agree to utilize defined standard technologies and a common set of identity management practices and identity attributes.

CLASSES OF MEMBERS

Federation Members may function as ***Identity Providers (IdPs)*** and/or as ***Service Providers (SPs)***. Identity and service providers have entered into a Federation Membership agreement with U. T. System under which they provide services that follow agreed-upon practices defined by the Federation Members.

RESPONSIBILITIES

1. *Identity Providers*

Multiple organizational units within a Member often determine the identities of individuals officially affiliated with a U.T. System institution. Examples may include the Human Resources Department, Office of the Registrar, Guest Authenticating Authority, etc. These units function as a "source of authority "(SOA) and provision "system of record" (SOR) databases that provide identity information to the Member's identity management (IdM) system. Identity providers manage two categories of identity -

- ***physical identity characteristics*** used to positively identify an individual (e.g. facial pictures, finger prints, etc.), and
- ***personal, often non-unique, attributes*** (e.g. given name, date of birth, place of birth, gender, netID, affiliations, certifications, etc.) often used for authorizations and provisioning of both internal and external applications.

A Member that is an Identity Provider (IdP) is responsible for:

a. Providing an authentication mechanism that offers some assurance that the same claimant is accessing a protected resource. ***When no identity proofing is associated with the issuance of a credential, the assurance associated with***

the presentation of the electronic credential is Level 1– i.e. the identity of the person is unverified.

b. Positively identifying persons for whom a U.T. institution assumes the responsibility of issuing certified identities.

c. Recording the unique identifying characteristics of each identified individual.

d. Assigning a single permanent U.T. institutional identifier to each positively identified person.

e. Registering each individual's permanent institutionally defined unique identifier.

f. Assigning additional unique identifier(s) that may be non-persistent but operationally required to each positively identified individual – e.g. a net ID.

g. Issuing each identified person a digital credential that is to be used by that individual to authenticate his or her identity

h. Providing Federation-approved Identity Services (e.g. Shibboleth) that Federation Members can rely on to

    i. authenticate a presenter's certified identity for access to services provided by Federation resource providers, and

    ii. to securely provide identity attributes known to be associated with an authenticated individual to Federation resource providers as specified by mutually agreed upon attribute release and acceptance policies.

i. Assuring accurate, timely binding of personal attribute information to identified and credentialed individuals having person entries in the Member's enterprise directory and any other attribute sources from which attributes are provided to relying parties as defined by attribute release policies.

j. Revoking or inactivating an individual's digital credential when

    i. a person having a Level 2, 3 or 4 credential no longer has an official relationship with that Member,

        1) An official relationship is defined by the policies and procedures governing the "source of authorities" (SOAs) that verify and register personal identities

    ii. the Member no longer accepts responsibility for providing an electronic identity for that person, or

iii. the Member is aware that the credential has become compromised or is no longer under the sole control of the person to whom it was issued.

k. Providing processes and tools that enable identity attributes to be maintained in a current state by appropriate systems and individuals.

2. Service Providers

Service Providers are the organizational units within Federation Members that manage electronic information resources which rely on Identity Providers (IdPs) managed by Federation Members for authentication and/or authorization assertions. Service providers are responsible for

a. *"knowing" the level of assurance (LOA) provided by Identity Providers:* Service Providers are responsible for determining if the LOA asserted by an IdP for the authenticated individual is appropriate for interacting with the Service Provider's relying resource. If an appropriate level of service is not provided by an IdP to meet security requirements of the SP, the Service Provider may need to implement its own identity management services in order to meet its security requirements.

b. *providing audit logs that enable investigation of security concerns related to information provided by Identity Providers.*

c. complying with Identity Provider standards and best practices for use and protection of identity information provided by IdPs to service provider applications.

d. providing contact information for individuals responsible for managing institutional services.

Service providers are responsible for implementing appropriate physical, network and host security, appropriate audit logs and service level descriptions.

MINIMUM REQUIREMENTS AND SERVICE LEVELS

Specific Requirements for Identity Providers

1. Each Federation Member's implementation of these minimum requirements and service levels as specified by the Federation must be audited subject to risk management decisions by that Member's internal audit department.

2. The identity of employees, residents and post-doctoral fellows must be verified by official hiring or acceptance procedures implemented by the Member, which must include in-person identity vetting.

3. The identity of students must be verified by official admission procedures implemented by the Member, which must include in-person identity vetting.

4. Guests or other officially approved affiliates must be verified by established procedures implemented by the Member, which must include in-person identity vetting.

5. Controlled values for the multi-valued, eduPersonAffiliation attribute include “faculty, student, staff, alum, member, affiliate and employee” However, individuals that are “affiliates” can only have that sole value assigned to the eduPersonAffiliation attribute.

6. Each organization unit with a Member that is responsible for determining an individual’s physical identity must submit that identity to a campus identity reconciliation process to ensure that an individual who may have been identified by multiple organizational units

   a. is assigned a single, permanent, unique identifier by the Member’s IdM process,

   b. has their vetted identity and assigned Member identifier permanently registered in the Member’s “Person Registry”

   c. is assigned a unique eduPersonPrincipalName (EPPN), and

   d. has only a single “person” entry in the Member’s Enterprise Directory.

7. If physical identities assigned to some individuals have not been verified according to the current Federation requirements, those identities must be re-verified prior to those individuals’ being approved to use the Federation.

8. The level of assurance a relying party has in a digital credential presented for authentication personal identity depends on

   a. the degree of confidence associated with the vetting process used to establish the identity of the individual to whom the credential was supposedly issued, and

   b. the degree of confidence that the individual who used the credential is the individual to whom the credential was appropriately issued - i.e. how resistant is the credential to tampering.

Credentialing of an identified individual by an IdP may be either in-person or remote.

- In-Person Credentialing

    - For university personnel and students, the credentialing authority must require a valid current primary Government Picture ID that contains the individual’s picture, and either address of record or nationality (e.g. driver’s license or passport), to verify that the individual to whom the credential is being issued is the intended recipient.

    - For guests or other affiliates, the credentialing authority must require at least one government-issued, picture ID and an additional ID that may be a non-picture ID. The second ID could be a non-expired credit card, a known employer issued ID, etc.

    - **Level 1:** An IdP must assert a **eduPersonAssurance attribute of “urn:mace:utsystem.edu:assurance:1”** for any individual whose identity was unverified but to whom a username/password credential was issued.

    - **Level 2:** An IdP may assert a **eduPersonAssurance attribute of “urn:mace:utsystem.edu:assurance:2”** for authentications by individuals whose physical identities were established by in-person vetting and were issued in person a username/password credential.

    - **Level 3:** An IdP may assert a **eduPersonAssurance attribute of “urn:mace:utsystem.edu:assurance:3”** for authentications by individuals whose physical identities were established by in-person vetting and were issued in person a two-factor credential that is protected by a cryptographic strength mechanism. Three kinds of tokens may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” tokens. These tokens protect against threats such as eavesdropping, replay, on-line guessing, verifier impersonation, and man-in-the-middle attacks.

    - **Level 4:** An IdP may assert a **eduPersonAssurance attribute of “urn:mace:utsystem.edu:assurance:4”** for authentications by individuals whose physical identities were established by in-person vetting and were issued in person a two-factor credential consisting of a "hard" token that cryptographically protects a key bound to the authentication process.

- Remote Credentialing

    - An IdP may remotely issue a username/password credential to an individual whose physical identity was previously vetted by an in-person appearance to that IdP's registration agent upon comparing information securely supplied by the intended recipient to validated data in a trusted database. The IdP must assert an **eduPersonAssurance attribute of "urn:mace:utsystem.edu:assurance:2"** for such an individual.

9. To provide interoperability with Service Providers, Identity Providers must implement specific attributes as required in the Federation document entitled *Common Identity Attributes*.

10. The security domain of scoped attributes such as EPPN should be the same as that of the IdP for all Federation members.

11. Authentication, attribute and other application services provided by an IdP must be secured as specified in the physical, network and host security policies implemented by that IdP as specified by UT System Information Resources Use and security Policy ("UTS 165").

12. Transmission of shared secrets such as a password during the credentialing or authentication processes must be protected by SSL 128 bit or greater encryption.

13. An ***Identity Provider service***, e.g. a Shibboleth IdP, may use one of several authentication services. Examples include:

    - ***Authentication services utilizing network transmitted passwords as an authentication credential*. (**It is critical that both IT personnel and users recognize that a network transmitted password is a user's digital credential and should be known only to the credential user).

        - **Network transmitted passwords can only support Level 1 or Level 2 assurance assertions.**

        - The network transmitted password authentication system should be as secure and simple to manage as possible –

preferably having only a single password change module and interface that handles all aspects of password changes.

  - Anytime a password is changed, the password change module should
    - log the institutional permanent identifier of the person whose password was changed,
    - log date and time of password change,
    - log the institutional permanent identifier of the individual who changed the password, and
    - send the password “owner” an e-mail stating when his/her password was changed and by whom.

- Any additional mechanisms for changing passwords must be identified and documented.

- Passwords and the controls used to limit on-line guessing attacks:

  - Shall ensure that an attack targeted against a selected user’s Password shall have a probability of success of less than 2^{-14} (i.e. one chance in 16,384) over the life of the password.
  - Additionally, a password shall have at least 10 bits of min-entropy (a measure of the difficulty that an attacker has to guess the most commonly chosen password used in a system) to protect against untargeted attack. *(Refer to NIST SP 800-63 Appendix A and the Credential Assessment Framework (CAF) Suite’s Entropy Spreadsheet to calculate resistance to online guessing)*
  - An example acceptable password would
    - have a minimum length of 8 characters,
    - contain a mix of upper and lower case alpha characters,
    - have at least 2 non-alpha characters (i.e. numerals and/or special characters), and
    - have a password life of 90 days.

- If possible, passwords should only be set/or reset by the identified person for whom the password is the assigned credential.

    - A password history must be maintained to prevent reuse of the current password as the new password.

    - Ideally, a network transmitted password management system should allow users also having an institutionally issued two-factor “soft” credential, “hard” credential or one-time password credential to set or change their network transmitted password.

    - If other designated individuals are permitted to change a user’s password,

        - The number of designated individuals must be kept at an absolute minimum.

        - A list of trained designees currently approved to set or change passwords must be maintained.

        - Any other individuals having system level privileges that would permit changing passwords or credential binding to user authentication must be maintained.

- ***Authentication services utilizing two-factor credentials.***

    - **Two-factor “soft” cryptographic credentials or one-time password credentials can be used to support Level 1, 2 and 3 assurance assertions.**

    - **Two-factor “hard” cryptographic credentials can be used to support Level 1, 2, 3 and 4 assurance assertions.**

    - Cryptographic credentials must be issued by each institution’s publicly rooted VeriSign certificate authority as specified by the U. T. System Master Service Agreement with VeriSign and the associated VeriSign Certificate Policy (CP) agreement and Certificate Practice Statement (CPS).

14. Processes and procedures must exist for immediately revoking or inactivating a digital credential when the Member becomes aware that a credential has been comprised.

15. Processes and procedures must exist to automatically revoke or inactivate a digital credential within 24 hours after an individual is no

longer officially affiliated with the Member as indicated by any institutional source of authority (SOA) database.

Specific Requirements for Service Providers

1. Services that rely on Federation Members that are Identity Providers must be compliant with all Member policies regarding privacy, security and application development.

2. Institutional Service Providers are responsible for the security of their applications and must implement any additional authentication measures required for the confidentiality and/or sensitivity of the application as well as data accessed by that application.

3. Service Providers must conduct appropriate usability and security testing of a relying service prior to the registration of that service with the Federation.

4. Service Providers must provide help desk support for the resolution of problems related to their applications. This support must be available to users located at Identity Provider Members as well as to those users who are students and employees of the Service Provider.

SYNCHRONIZATION WITH REPOSITORIES OF RECORD

1. Processes must exist that maintain close synchronization of identity information in the identity management system with corresponding source records in the institutional source of authority (SOA) databases. Changes in the SOA databases should be reflected in the identity management repositories within 24 hours or sooner.

USER INTERFACE DESIGN

1. There exists a certain amount of “bouncing” of Federation users among identity providers, service providers, and the “Where Are You From” (WAYF) server that is inherent in the current technology. Efforts should be made to reduce this confusion.

2. Members should structure login processes to interact with the **UT System IdM Federation** WAYF to declare the “origin” institution without user interaction later in the session.

3. Clearly indicate that the help desk should be contacted for problems that may occur at each step.

4. Both Service Providers and Identity Providers should conduct usability studies to identify confusing aspects of their user interfaces.

TECHNICAL SPECIFICATIONS

Members of the Federation must be capable of exchanging attribute information with other members of the Federation via protocol and standards implemented by Shibboleth version 1.2 or higher. The X.509 SSL server certificates used to authenticate institutional Shibboleth servers must be issued by the U. T. System Office of Technology and Information Services issued under the Master Services Agreement with VeriSign.

REFERENCES

Credential Assessment Framework (CAF) Suite, E-Authentication Initiative, 2005

Entropy Spreadsheet, v2.0.0

Electronic Authentication Guideline. William E. Burr, Donna F. Dodson, Timothy Polk. National Institute of Standards and Technology – U.S. Department of Commerce. September 2004.

Entropy Spreadsheet, v2.0.0

Establishment of E-Authentication Service Component, Federal Register, Vol. 70, No. 150, August 5, 2005

Personal Identity Verification (PIV) of Federal Employees and Contractors. Federal Information Process Standards Publications (FIPS PUB 201), National Institute of Standards and Technology, February 25, 2005.