Guidelines for Determining the

Level of Assurance of Personal Digital Identities

Determining the level of authentication assurance (LOA) placed in a personal digital identity required to access specific applications and transactions involves evaluating the risk and impact of an *authentication error*. Authentication error is the misuse of credentials, either malicious or unintentional, where the person using a credential is not the person to whom the credential was issued. The steps in the methodology below are modeled on steps from OMB M-04-04, E-Authentication Guidance for Federal Agencies, and the National Institute of Standards and Technology Special Publication 800-63, Electronic Authentication Guideline.

The steps are summarized below and are detailed in the Steps section.

1. Determine the potential impact of an authentication error.
    a. Consider the consequences of an authentication error.
    b. Assign an impact value to each type of consequence.
    c. Determine the potential impact profile.
2. Map the potential impact of an authentication error to the level of assurance of the personal digital identity.
3. Select the *digital credential*(s) appropriate to the level of assurance.
4. Implement digital credential(s.)
5. Prior to production deployment, validate that the implemented system has achieved the required assurance level, including a security assessment.
6. Reassess the system, evaluating changes in risk and technology.

Steps

These steps should be completed to determine the appropriate authentication credentials for systems and applications that allow electronic access by Virginia Tech affiliates.

1. Determine the potential impact of an authentication error.

1.a Consider the consequences of authentication error

The following security issues must be considered when evaluating the consequences of an authentication error.

- Loss of confidentiality: unauthorized user views protected information
- Loss of integrity: unauthorized user changes information
- Loss of availability: unauthorized user prevents others from using a service

Because an authentication error may lead to the wrong individuals viewing or retrieving sensitive information, changing university information, approving important actions (for example, spending university funds), or accessing electronically protected assets, negative consequences may ensue. The following negative consequences should be considered.

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or liability to the university or to individuals using the application (For example, identity theft could result in financial loss.)
- Harm to university programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Penalties for civil, criminal, or disciplinary violations

1.b Assign an impact value

If an authentication error were to occur, what would be its impact? Consider that the burden of negative consequences may be borne by a single university unit, but more often by the university as a whole. The burden may also be borne by one or more of its many community members.

Each applicable type of consequence may have one of four impact values—low, moderate, high, or very high:

- **Low** impacts cause inconvenience without lasting effects. An authentication error with low impact would not involve financial, physical, or reputational harm to the university or to its employees, students, business partners, or friends.
- **Moderate** impacts have more serious effects, either for the university or for members of the university community. Moderate impacts are serious short-term or limited long-term.
- **High** impacts have severe adverse effects resulting in serious long-term damage.
- **Very high** impacts are catastrophic or life-threatening, with very serious, unrecoverable/irreversible long-term impact.

After assigning impact values to each type of consequence, determine whether any additional controls can be applied to reduce the likelihood of authentication error occurring, the severity of the consequences, or the magnitude of impact.

Examples of additional controls:

- Educating users to safeguard their credentials and select strong passwords
- Requiring multiple people to approve or execute transactions
- Notifying individuals of changes to information
- Monitoring transaction logs

Iterations of this process are possible.

1.c Determine the potential impact profile

The next step is to determine the *potential impact profile* (Table 1).

Table 1: Potential impact profile levels[1]

Consequences	Potential Impact Profile Levels					
	0	1	2	3	4	5
Inconvenience, distress, or damage to standing or reputation	N/A	Low	Mod	Mod	High	Very high
Financial loss or university liability	N/A	Low	Mod	Mod	High	Very high
Harm to university programs or public interests	N/A	N/A	Low	Mod	High	Very high
Unauthorized release of sensitive information	N/A	N/A	Low	Mod	High	Very high
Personal safety	N/A	N/A	N/A	Low	Mod (or) High	Very high
Penalties for civil, criminal, or disciplinary violations	N/A	N/A	Low	Mod	High	Very high

Example: Upon request from the Dean of Students, an application was developed to allow university personnel to report student behavior that they suspect might lead to the student harming him/herself or another member of the university community. Reports are intended to be accessed only by members of the threat assessment team for review and evaluation.

In analyzing the potential impact of an authentication error, the results were:

Inconvenience, distress or damage to standing or reputation—High
Financial loss or university liability—High
Harm to university programs or public interests—Moderate
Unauthorized release of sensitive information—High
Personal safety—High
Penalties for civil, criminal, or disciplinary violations—High

Table 1 Example: Potential impact profile levels of the student behavior reporting system

Consequences	Potential Impact Profile Levels					
	0	1	2	3	4 ✔	5
Inconvenience, distress or damage to standing or reputation	N/A	Low	Mod	Mod	(High)	Very high
Financial loss or university liability	N/A	Low	Mod	Mod	(High)	Very High
Harm to university programs or public interests	N/A	N/A	Low	(Mod)	High	Very High
Unauthorized release of sensitive information	N/A	N/A	Low	Mod	(High)	Very high
Personal safety	N/A	N/A	N/A	Low	Mod (or) (High)	Very high
Penalties for civil, criminal, or disciplinary violations	N/A	N/A	Low	Mod	(High)	Very High

Table 1: The potential impacts range from Level 3 to Level 4, so the highest -- Level 4 -- must be selected.

The highest impact profile level from Table 1 is selected. In cases where multiple profiles from Table 1 apply, consider context in choosing the appropriate profile level. Additional guidelines and examples are provided in OMB M-04-04, E-Authentication Guidance for Federal Agencies.

[1] Foundation document: OMB M-04-04, E-Authentication Guidance for Federal Agencies

2. Map the potential impact profile to a level of assurance.

The level of assurance (LOA) of a personal digital identity is a number that represents the degree of confidence that the person who presents a digital credential representing an identity is, in fact, that person. LOAs used at Virginia Tech are described in the "Standard for Use of Personal Digital Identities." They range from 0—no assurance—to 5—very high assurance.

Mapping the impact of an authentication error to the level of assurance in the personal digital identity requires relating the potential impact profile level from Table 1 to the levels of assurance in Table 2. Typically, there is a one-to-one correspondence between the potential impact profile level and the personal digital identity LOA. As the impact of authentication error increases, a higher level of assurance in the personal digital identity is required. Additional considerations include the following:

- If there is any impact at all, some form of authentication is required. (LOA 0 is not appropriate.)
- When individual accountability is necessary, LOA 3 or higher must be used.
- If individual accountability is necessary and includes elements of non-repudiation, LOA 4 or higher is required.
- If a system supports multiple, separately authenticated functions, it is possible to map each function to a different personal digital identity LOA.

In the example above, the level 4 potential impact profile maps to personal digital identity LOA 4 in Table 2 below.

Table 2: Levels of assurance of personal digital identities[2]

LOA	Characteristics of personal digital identities			
	Identity assertion	**Identity proofing requirements**	**Authentication factors**	**Virginia Tech centrally managed identities**
0	No identity is asserted.	None	None	N/A
1	Little or no confidence in the validity of the asserted identity	Some identity information is acquired. Little or no verification is performed.	Single-factor authentication	• GAMS guest account and password • NetCert
2	Some confidence that the asserted identity is valid	Some identity information is acquired, with some level of verification.	Single-factor authentication	• PID and password • Hokies ID and password • Oracle ID and password • Hokie Passport card • VASCO DigiPass Go 6 one-time password device
3	Moderate degree of confidence in the validity of the asserted identity	Matching of the collected identity information is strengthened by additional identity verification from a trusted authority. Identity proofing may be in-person or, in some circumstances, remote.	A minimum of two authentication factors is required; i.e., something you know and (something you have or something you are). Cryptographic keys may be stored in software.	One of several solutions is the ID and password used in conjunction with a personal digital certificate (PDC) key stored in software, planned for implementation at Virginia Tech Fall, 2012.
4	High degree of confidence in the validity of the asserted identity	In-person identity proofing is required, including referencing a biometric attribute.	A minimum of two authentication factors is required. Cryptographic keys must be stored on a *hardware token* that does not allow the export of authentication keys.	• Virginia Tech personal digital certificate (PDC) on SafeNet eToken • Vasco DigiPass Go 6 one time password device plus corresponding PID/ password

[2] Foundation document: the National Institute of Standards and Technology Special Publication 800-63-1, Electronic Authentication Guideline

LOA	Characteristics of personal digital identities			
	Identity assertion	**Identity proofing requirements**	**Authentication factors**	**Virginia Tech centrally managed identities**
5	Very high degree of confidence in the validity of the asserted identity	In-person identity proofing is required, including recording a biometric attribute.	Three authentication factors are required, including a biometric attribute and a cryptographic key stored on a hardware token that meets certain technical specifications.	Virginia Tech PDC on SafeNet eToken plus confirmation that an individual's appearance matches his/her Hokie Passport photo

3. Select the digital credentials appropriate to the level of assurance.

Personal digital identities are represented to electronic services by *digital credentials*. The type of credential used to access the service must match the LOA of the personal digital identity it represents.

Table 2 includes examples of Virginia Tech *enterprise credentials*; namely, guest accounts (LOA 1), PIDs, Hokies IDs, and Oracle/Banner IDs (all LOA 2), and Virginia Tech personal digital certificates (LOA 4 if the private key is stored on an eToken). Using enterprise credentials provides an established LOA (from Table 2) and ensures a secure repository for the credentials. Any department- or unit-based credentials that are used must be mapped to a LOA and kept in a secure repository.

Identity Management Services (IMS) provides expertise on identity management concepts and practices, including considerable knowledge regarding digital credentials supported at Virginia Tech. IMS will assist in affirming characteristics of personal digital identities, and in selecting corresponding credentials. IMS will also assist in seeking input and approval, if needed, from data stewards

4. Implement digital credentials.

Although the sponsor is responsible for overseeing implementation of the personal digital credentials, IMS will provide assistance during the implementation phase. Authentication methods vary, depending on the credentials being used. Web applications using PID should utilize the *Central Authentication Service* (CAS) or *Shibboleth*. Authentication using the Virginia Tech PDC on an eToken is accomplished with CAS or client SSL. Virginia Tech's implementation of CAS can pass attributes for authorization and level of assurance to the CAS-enabled application. Thus, a CAS-enabled application can detect the LOA of certain Virginia Tech enterprise credentials. See the Middleware CAS wiki for more information.

Some externally hosted web applications support authentication with Shibboleth. Virginia Tech maintains a Shibboleth Identity Provider and is a member of the InCommon federation. See the Middleware Shibboleth wiki for more information.

Centrally managed Microsoft credentials are incorporated into an Active Directory infrastructure that utilizes several levels of authentication and authorization to provide security as well as backwards compatibility. Virginia Tech functions requiring Hokies Active Directory accounts for authentication must use NTLMv2, Kerberos or LDAPS. Active Directory integration is built into most Microsoft applications. Web-based Windows applications may also take advantage of CAS.

5. Validate that the implemented system has achieved the required assurance level, including a security assessment.

As a part of the implementation of personal digital identities, the Information Technology Security Office will assist with a security assessment.

6. Reassess the system.

As changes relate to authentication, reassessment of impact and levels of assurance of digital identities should be done.

Definitions

Authentication is the process of establishing confidence in the identity of users of online processes. Authentication normally involves comparing digital credential items to information that has been previously stored.

Authentication error is the misuse of credentials, either malicious or unintentional, where the person using a credential is not the person to whom the credential was issued.

Authentication factors are elements that are used in forming digital credentials to verify a person's identity. The number of different factors used for authentication is directly related to the level of trust a process can place in the validity of the digital credential. As the number of factors increases, so does the level of trust in the credential. Factors include

a. "something you know" (e.g., a password, passphrase, or PIN, or other information),
b. "something you have" (e.g., an ATM card, a USB device, a digital certificate),
c. "something you are" (biometric attribute such as a finger print or typing pattern).

Note that multiple items within a given factor do not increase the number of factors.

Biometric attributes represent measurable biological or behavioral characteristics of a person, which can be used in verifying identity. Fingerprints, iris patterns, facial images and voice patterns are examples of biological biometrics. Typing patterns are behavioral biometrics.

Central Authentication Service (CAS) is a central logon service that enables single sign-on and provides authentication without revealing a person's password to the application that requires authentication.

Digital credentials refer to the identifying character strings, digital certificates, passwords, PINs, and other means of representing an asserted identity to an online process.

Electronic services In this standard, the term "electronic services" is used to refer to the broad scope of resources that rely on identifying individuals seeking access to those resources. Included are online systems, services, and applications; functions within those online systems, services, and applications; and physical resources and facilities.

Enterprise credentials are managed centrally and are available to Virginia Tech affiliates. Enterprise credentials may not be available to all types of Virginia Tech affiliates.

Hardware token is a physical device such as a USB fob or smart card, typically small enough to be carried in a pocket or purse. The device is used as an authentication factor to help prove that a person is who he/she claims to be.

Identity assertion Individuals may claim or assert that they are a particular identity. This assertion may or may not be deemed true or accurate, and may or may not be matched to identity information that has been gathered.

Identity information acquisition is the collection of information that provides the required level of certainty that a real-world identity exists. Examples include collecting transcripts for potential students, references for potential employees, and e-mail addresses for potential guests. Identity information during the acquisition phase may be retained in the identity management system for future use in identity proofing.

Identity proofing is the process by which a specific identity subject is matched with the identity information acquired and retained in the identity management system. The subject's eligibility for an institutional personal digital identity is often evaluated during the identity-proofing phase.

Level of assurance (LOA) is the degree of confidence that the person who presents a digital credential representing an identity is, in fact, that person. Specifically, the LOA represents a degree of certainty that 1) a person's identity was adequately verified before a set of digital credentials was issued to that person and 2) the credentials are used only by the person to whom they were issued.

Personal digital identity is a person's asserted personal identity—typically name with associated attributes—along with the digital credentials that represent that identity in an online environment. The personal digital identity of a person is his or her online representation of a real-world identity. As a process, using personal digital identities consists of:

- *Identity information acquisition*
- Identity proofing
- Issuance of digital credentials
- Using the digital credentials for online authentication

Potential impact profile is the result of a method that links consequences of authentication error to an impact level.

Processes that rely on electronic authentication Some examples are Hokie Mart entries and approvals, e-mail, university payroll, submitting grades, buying a parking pass online, online leave reporting, downloading university letterhead, submitting Virginia Tech Daily News.

Risk is the net negative impact of the exploit of a vulnerability, considering both the probability and the impact of occurrence.[3]

Security assessments are conducted by the Information Technology Security Office upon request, or as required by policy or law, to verify a secure operating environment.

Shibboleth is a standards-based open source software package that supports federated identity management and allows services provided by other institutions to authenticate and authorize individuals securely and with appropriate protection of confidentiality. A Shibboleth service provider recognizes credentials local to the institution with which the user is affiliated rather than requiring the user to establish a credential unique to the service. See the Middleware Shibboleth Wiki for more information.

A **sponsor** is the person or group responsible for making policy and/or technical decisions for a system, application, or functional component. If an application is a deliverable in a project, the project sponsor is typically the application sponsor.

References

Virginia Tech User Certification Authority Certification Practices Statement, http://www.pki.vt.edu/vtuca/cps/index.html

Standard for Use of Personal Digital Identities; http://www.it.vt.edu/administration/policies.html

Policy 7040, Personal Credentials for Enterprise Electronic Services; http://www.policies.vt.edu/7040.pdf

National Institute of Standards and Technology Special Publication 800-63, Electronic Authentication Guideline; http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems; http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules; http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[3] National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems

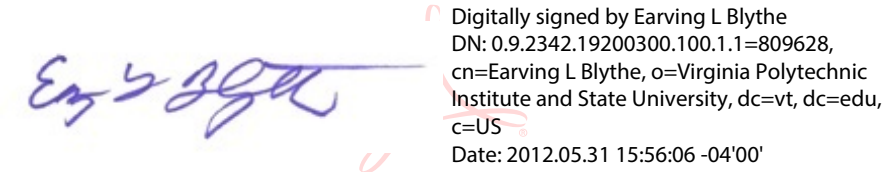
OMB M-04-04, E-Authentication Guidance for Federal Agencies;
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

University of Wisconsin, Madison, User Authentication and Levels of Assurance;
http://www.cio.wisc.edu/security/initiatives/levels.aspx

Virginia Tech, Central Authentication Service;
http://www.middleware.vt.edu/doku.php?id=middleware:cas

Virginia Tech, Shibboleth; http://www.middleware.vt.edu/doku.php?id=middleware:shib

Approved by:



Earving L. Blythe