June 9, 2010

Standard for Personal Digital Identity Levels of Assurance

Many university resources – certain electronic information and protected physical spaces – must not be accessed by unauthorized individuals. *Personal digital identities* allow people to assert their identities to *electronic services*, thereby enabling authorized access to the service, and preventing unauthorized access.

In accordance with the "Information Technology Security and Authority Resolution" of June 4, 2007, http://www.bov.vt.edu/minutes/07-06-04minutes/attach_v_070604.pdf, the Vice President for Information Technology and Chief Information Officer establishes this Standard for Personal Digital Identity Levels of Assurance.

Italicized words and phrases are defined in section 3.

1. Purpose

The purpose of this standard is to designate the *levels of assurance* for personal digital identities used at Virginia Tech.

1.1 Personal digital identity

A personal digital identity is an online representation of a real-world identity. A personal digital identity is a person's asserted identity—typically name with associated attributes—along with the *digital credentials* that represent that identity in an online environment. When used for online approvals and digital signatures, a personal digital identity reflects a level of trust in a person's identity.

In online systems, access to protected resources is controlled by requiring people to present digital credentials before access is granted. If the person presenting those credentials is not the person to whom the credential was issued, an authentication error occurs. Implementing an appropriate personal digital identity can mitigate the risk of authentication error and enhances security by helping to ensure that access to a particular university resource is granted to, and only to, the intended individual(s).

1.2 Level of assurance

The level of assurance (LOA) of a personal digital identity is the degree of confidence that the person who presents a digital credential representing an identity is, in fact, that person. The degree of confidence is tied to the rigor used to ascertain the individual's identity before a credential is issued, and also to the security of the credential. Each level of assurance is characterized by

- an *identity assertion*,
- *identity proofing* requirements, and
- *authentication factors*.

An identity assertion is a claim to be a particular "real world" person. Identity proofing requirements refer to the processes by which the credential issuer validates sufficient information to uniquely identify the person applying for a credential. Authentication factors refer to controls that seek to ensure that the claimed and proofed identity is the same as the identity being presented in an online setting.

In the lowest level of assurance, level 0, no identity is being claimed or asserted. Some online services may use identifiers and passwords, but without any requirement to uniquely identify the user. Often, no identifier or identity is used at all, as is the case with open websites.

In level 1, there is some claim to an identity. One example is when an e-mail address is used as the identity assertion: "I am this e-mail address." My presentation of an e-mail address is verification that I have the ability to access information at that e-mail address.

For level 2 and higher levels, the claim to a real world identity is stronger, and accompanied by more information used for identity proofing. At the higher levels, reliance on other identity providers is also commonly used—in-person presentation of one or more photo IDs from a reliable authority like a state or national government is common.

Authentication factors refer to the type of information used to verify a person's identity in the online/electronic environment. 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).

2. Virginia Tech levels of assurance

Virginia Tech classifies personal digital identity LOAs into six tiers from 0 through 5. These levels are modeled on the National Institute of Standards and Technology (NIST) Special Publication 800-63, where Virginia Tech's levels 1-4 reflect criteria from NIST levels 1-4.The chart below designates the Virginia Tech LOAs with a description of the identity assertion, identity-proofing requirements, and authentication factors for each level.

LOA	Characteristics of personal digital identities		
	Identity assertion	**Identity-proofing requirements**	**Authentication factors**
0	No identity is asserted.	None	None
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
2	Some confidence that the asserted identity is valid	Some identity information is acquired, with some level of verification.	Single-factor authentication
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.
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 physical device that does not allow the export of authentication keys.
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.

3. Definitions

Authentication error is the misuse of credentials, either malicious or intentional, 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.

Digital credentials are the identifying character strings, plus authentication factors, that are presented to authenticate a person to electronic services.

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.

An **identity assertion** is the claim by an individual that he or she is 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 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.

The **level of assurance** is the degree of confidence that the person who presents a digital credential representing an identity is, in fact, that person.

A **personal digital identity** is an online representation of a real-world identity. A personal digital identity is a person's asserted identity—typically name with associated attributes—along with the digital credentials that represent that identity in an online environment. When used for online approvals and digital signatures, a personal digital identity reflects a level of trust in a person's identity.

4 References

Information Technology Security and Authority Resolution, http://www.bov.vt.edu/minutes/07-06-04minutes/attach_v_070604.pdf, June 4, 2007

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

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

NIST Special Publication 800-63, Version 1.0.2, Electronic Authentication Guide, http://csrc.nist.gov/publications/nistpubs/index.html

Approval

Approved, Vice President for Information Technology and Chief Information Officer, Earving L. Blythe

(Signed) Earving L Blythe Digitally signed by Earving L Blythe DN: dc=edu, dc=vt, c=US, o=Virginia Polytechnic Institute and State University, cn=Earving L Blythe, 0.9.2342.19200300.100.1.1=809628, serialNumber=1231 Date: 2010.06.16 17:31:10 -04'00'

Date _____