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 Virginia Tech Board of Visitors' "Information Technology Security and Authority Resolution" of June 4, 2007, 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

A *level of assurance (LoA)* is an ordinal measure of strength, robustness, or validity. The security of an online authentication event using a personal digital identity is evaluated based on levels of assurance of the following components:

- identity proofing
- the authentication process, including *authenticators*
- the assertion protocol of the federation, if applicable

2. Scope

Identity proofing requirements refer to the processes by which the credential issuer validates sufficient information to uniquely identify the person applying for a credential. The authentication process seeks to ensure that the claimed and proofed identity is the same as the identity being presented in an online setting.

Each of these components has is own level of assurance or degree of confidence, and is aligned with NIST Special Publication 800-63-3.[1]

Identity Assurance Level	
IAL1	No identity proofing required. Attributes, if any, are self-asserted.
IAL2	Either remote or in-person identity proofing, with identifying attributes verified against previously-collected online data.
IAL3	In-person identity proofing required, with identifying attributes verified through examination of physical documentation such as one or more photo IDs from a reliable authority like a state or national government..

Figure 1: Identity Assurance Level

Authenticator Assurance Level	
AAL1	Single factor authentication, with some assurance that the claimant controls the authenticator. A secure authentication protocol is required. Example: passphrase.
AAL2	Two different authentication factors, demonstrating high confidence that the claimant controls the authenticator(s) registered to the subscriber. Example: passphrase plus Duo with any of the Virginia Tech-supported authentication methods.
AAL3	Two different authentication factors, demonstrating very high confidence that the claimant controls the authenticator. Cryptographic protocols are required to prove possession of a “hard” authenticator that provides resistance to impersonation. Example: passphrase plus Duo with mobile app PUSH, YubiKey, or D-100.

Figure 2: Authentication Assurance Level

[1] Definitions and figures are derived or reproduced from NIST SP 800-63-3.

3. Standard: Virginia Tech combined levels of assurance

While Virginia Tech allows flexibility in combining assurance levels for identity proofing and authentication, certain levels are required when accessing *high risk data*. The chart below designates the Virginia Tech combinations.

Virginia Tech Combined Assurance Levels			
	AAL1	AAL2	AAL3
IAL1: Without high risk data	Allowed	Allowed	Allowed
IAL1: With high risk data	NO	Allowed	Allowed
IAL2	NO	Allowed	Allowed
IAL3	NO	Allowed	Allowed

Figure 3: Virginia Tech Combined Assurance Levels

---

4. 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 *something you know, something you have,* and *something you are.* Every authenticator has one or more authentication factors. As the number of factors increases, so does the level of trust in the credential.

Authenticator is something a person controls and possesses -- typically a passphrase or cryptographic module -- that is used to verify identity as a prerequisite to allowing access to an online resource.

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.

High risk data pertains to data where protection of the data is required by law or regulation and Virginia Tech is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed. See Standard for High Risk Digital Data Protection .

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.

5. References

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

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

Virginia Tech Standard for High Risk Digital Data Protection
https://it.vt.edu/content/dam/it_vt_edu/policies/Standard-for-High-Risk-Digital-Data-Protection.pdf

This version of the standard has been updated to align appropriately with the latest iteration (12-1-2017) of the NIST Special Publication 800-63-3, Digital Identity Guidelines
https://csrc.nist.gov/publications/detail/sp/800-63/3/final

6. Maintenance of Standard

The Secure Identity Services unit is responsible for this IT Standard. Questions may be directed to rhach@vt.edu.