COMMONWEALTH OF VIRGINIA

~~Information Technology Resource Management~~IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (~~ITRM~~IMSAC)

REFERENCE DOCUMENT
National Institute of Standards and Technology (NIST)
Assurance Model

1 Terminology and Definitions

The IMSAC guidance document series applies a standards-based terminology and definitions for core concepts in the digital identity management domain. The IMSAC terminology satisfies three primary requirements for the Commonwealth's minimum specification: (1) aligns with the National Institute of Standards and Technology Special Publication 800-63-3, which sets federal guidelines for digital authentication and identity management; (2) complies with terminology codified under the Electronic Identity Management Act (§ 59.1-550); and (3) remains consistent with terminology published by standards development organizations (SDOs) in the global identity ecosystem.

The IMSAC terminology consists of the following definition sets:

- National Institute of Standards and Technology Special Publication 800-63-3
  https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3
- Electronic Identity Management Act, § 59.1-550. Definitions, *Code of Virginia*
  http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/
- International Telecommunication Union. Recommendation X. 1255: *Framework for Discovery of Identity Management Information* (Non-Person Entities)
  http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11951&lang=en

The IMSAC terminology and definitions also may be accessed at:
http://vita.virginia.gov/default.aspx?id=6442475952

~~Terms used in this document comply with definitions in the Public Review version of the National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3), and align with adopted definitions in § 59.1-550, *Code of Virginia*, and the Commonwealth of Virginia's ITRM Glossary (ITRM Glossary).~~[1]

~~Active Attack: An online attack where the attacker transmits data to the claimant, credential service provider, verifier, or relying party. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking.~~

~~Address of Record: The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office box number, Fleet Post Office box number or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available.~~

~~[1] NIST SP 800-63-3 may be accessed at https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3 . At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.~~
~~§ 59.1-550, *Code of Virginia*, may be accessed at http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550/~~
~~The Commonwealth's ITRM Glossary may be accessed at~~
~~http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/PSG_Sections/COV_ITRM_Glossary.pdf~~

Approved: Federal Information Processing Standard (FIPS) approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation.

Applicant: A party undergoing the processes of registration and identity proofing.

Assertion: A statement from a verifier to a relying party (RP) that contains identity information about a subscriber. Assertions may also contain verified attributes.

Assertion Reference: A data object, created in conjunction with an assertion, which identifies the verifier and includes a pointer to the full assertion held by the verifier.

Assurance: In the context of [OMB M-04-04][2] and this document, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Asymmetric Keys: Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Attack: An attempt by an unauthorized individual to fool a verifier or a relying party into believing that the unauthorized individual in question is the subscriber.

Attacker: A party who acts with malicious intent to compromise an information system.

Attribute: A claim of a named quality or characteristic inherent in or ascribed to someone or something.

Authentication: The process of establishing confidence in the identity of users or information systems.

Authentication Protocol: A defined sequence of messages between a claimant and a verifier that demonstrates that the claimant has possession and control of a valid authenticator to establish his/her identity, and optionally, demonstrates to the claimant that he or she is communicating with the intended verifier.

Authentication Protocol Run: An exchange of messages between a claimant and a verifier that results in authentication (or authentication failure) between the two parties.

[2] [OMB M-04-04] Office of Management and Budget, Memorandum 04-04: E-Authentication Guidance for Federal Agencies, accessible at https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.

Authentication Secret: A generic term for any secret value that could be used by an attacker to impersonate the subscriber in an authentication protocol. These are further divided into short-term authentication secrets, which are only useful to an attacker for a limited period of time, and long-term authentication secrets, which allow an attacker to impersonate the subscriber until they are manually reset. The authenticator secret is the canonical example of a long term authentication secret, while the authenticator output, if it is different from the authenticator secret, is usually a short term authentication secret.

Authenticator: Something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. In previous versions of this guideline, this was referred to as a token.

Authenticator Assurance Level (AAL): A metric describing robustness of the authentication process proving that the claimant is in control of a given subscriber's authenticator(s).

Authenticator Output: The output value generated by an authenticator. The ability to generate valid authenticator outputs on demand proves that the claimant possesses and controls the authenticator. Protocol messages sent to the verifier are dependent upon the authenticator output, but they may or may not explicitly contain it.

Authenticator Secret: The secret value contained within an authenticator.
Authenticity: The property that data originated from its purported source.

Bearer Assertion: An assertion that does not provide a mechanism for the subscriber to prove that he or she is the rightful owner of the assertion. The RP has to assume that the assertion was issued to the subscriber who presents the assertion or the corresponding assertion reference to the RP.

Bit: A binary digit: 0 or 1.

Biometrics: Automated recognition of individuals based on their behavioral and biological characteristics. In this document, biometrics may be used to unlock authenticators and prevent repudiation of registration.

Certificate Authority (CA): A trusted entity that issues and revokes public key certificates.

Certificate Revocation List (CRL): A list of revoked public key certificates created and digitally signed by a Certificate Authority. [RFC 5280][3]

Challenge-Response Protocol: An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a secret (such

[3] [RFC 5280] Official Internet Protocol Standards, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008, accessible at http://www.rfc-editor.org/info/rfc5280.

as by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the claimant possesses and controls the secret.

Claimant: A party whose identity is to be verified using an authentication protocol.

Claimed Address: The physical location asserted by an individual (e.g. an applicant) where he/she can be reached. It includes the residential street address of an individual and may also include the mailing address of the individual. For example, a person with a foreign passport, living in the U.S., will need to give an address when going through the identity proofing process. This address would not be an "address of record" but a "claimed address."

Claimed Identity: A declaration by the applicant of their current Personal Name, date of birth and address. [GPG45][4]

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA): An interactive feature added to web forms to distinguish use of the form by humans as opposed to automated agents. Typically, it requires entering text corresponding to a distorted image or from a sound stream.

Cookie: A character string, placed in a web browser's memory, which is available to websites within the same Internet domain as the server that placed them in the web browser.

Credential: An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to an authenticator possessed and controlled by a subscriber. While common usage often assumes that the credential is maintained by the subscriber, this document also uses the term to refer to electronic records maintained by the CSP which establish a binding between the subscriber's authenticator(s) and identity.

Credential Service Provider (CSP): A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.

Cross Site Request Forgery (CSRF): An attack in which a subscriber who is currently authenticated to an RP and connected through a secure session, browses to an attacker's website which causes the subscriber to unknowingly invoke unwanted actions at the RP. For

[4] [GPG 45] UK Cabinet Office, Good Practice Guide 45, Identity proofing and verification of an individual, November 3, 2014, accessible at https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual.

~~example, if a bank website is vulnerable to a CSRF attack, it may be possible for a subscriber to unintentionally authorize a large money transfer, merely by viewing a malicious link in a webmail message while a connection to the bank is open in another browser window.~~

~~Cross Site Scripting (XSS): A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user supplied data from requests or forms without sanitizing the data so that it is not executable.~~

~~Cryptographic Key: A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, key requirements shall meet the minimum requirements stated in Table 2 of NIST SP 800-57 Part 1. See also Asymmetric keys, Symmetric key.~~

~~Cryptographic Authenticator: An authenticator where the secret is a cryptographic key.~~

~~Data Integrity: The property that data has not been altered by an unauthorized entity.~~

~~Derived Credential: A credential issued based on proof of possession and control of an authenticator associated with a previously issued credential, so as not to duplicate the identity proofing process.~~
~~Digital Signature: An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation.~~

~~Eavesdropping Attack: An attack in which an attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the claimant.~~

~~Electronic Authentication: The process of establishing confidence in user identities electronically presented to an information system.~~

~~Entropy: A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits.~~

~~Extensible Mark-up Language (XML): Extensible Markup Language, abbreviated XML, describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them.~~

~~Federal Bridge Certification Authority (FBCA): The FBCA is the entity operated by the Federal Public Key Infrastructure (FPKI) Management Authority that is authorized by the Federal PKI Policy Authority to create, sign, and issue public key certificates to Principal CAs.~~

Federal Information Security Management Act (FISMA): Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Federal Information Processing Standard (FIPS): Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.[5]

Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:

- (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and
- (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.

Holder-of-Key Assertion: An assertion that contains a reference to a symmetric key or a public key (corresponding to a private key) held by the subscriber. The RP may authenticate the subscriber by verifying that he or she can indeed prove possession and control of the referenced key.

Identity: A set of attributes that uniquely describe a person within a given context.

Identity Assurance Level (IAL): A metric describing degree of confidence that the applicant's claimed identity is their real identity.

Identity Proofing: The process by which a CSP and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person.

Kerberos: A widely used authentication protocol developed at MIT. In "classic" Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a "ticket" by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to- KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users.

[5] Federal Information Processing Standard (FIPS), accessible at http://www.nist.gov/itl/fips.cfm.

~~Knowledge-Based Authentication: Authentication of an individual based on knowledge of information associated with his or her claimed identity in public databases. Knowledge of such information is considered to be private rather than secret, because it may be used in contexts other than authentication to a verifier, thereby reducing the overall assurance associated with the authentication process.~~

~~Man-in-the-Middle Attack (MitM): An attack on the authentication protocol run in which the attacker positions himself or herself in between the claimant and verifier so that he can intercept and alter data traveling between them.~~

~~Message Authentication Code (MAC): A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non-repudiation protection.~~

~~Multi-Factor: A characteristic of an authentication system or an authenticator that uses more than one authentication factor. The three types of authentication factors are something you know, something you have, and something you are.~~

~~Network: An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties. Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e., eavesdropping) attack at any point between the parties (e.g., claimant, verifier, CSP or RP).~~

~~Nonce: A value used in security protocols that is never repeated with the same key. For example, nonces used as challenges in challenge-response authentication protocols must not be repeated until authentication keys are changed. Otherwise, there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.~~

~~Off-line Attack: An attack where the attacker obtains some data (typically by eavesdropping on an authentication protocol run or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing.~~

~~Online Attack: An attack against an authentication protocol where the attacker either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel.~~

~~Online Guessing Attack: An attack in which an attacker performs repeated logon trials by guessing possible values of the authenticator output.~~

~~Passive Attack: An attack against an authentication protocol where the attacker intercepts data traveling along the network between the claimant and verifier, but does not alter the data (i.e., eavesdropping).~~

~~Password: A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.~~

~~Personal Identification Number (PIN): A password consisting only of decimal digits.~~

~~Personal Identity Verification (PIV) Card: Defined by [FIPS 201] as a physical artifact (e.g., identity card, smart card) issued to federal employees and contractors that contains stored credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).~~

~~Personally Identifiable Information (PII): As defined by OMB Circular A-130, Personally Identifiable Information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.~~

~~Pharming: An attack in which an attacker corrupts an infrastructure service such as DNS (Domain Name Service) causing the subscriber to be misdirected to a forged verifier/RP, which could cause the subscriber to reveal sensitive information, download harmful software or contribute to a fraudulent act.~~

~~Phishing: An attack in which the subscriber is lured (usually through an email) to interact with a counterfeit verifier/RP and tricked into revealing information that can be used to masquerade as that subscriber to the real verifier/RP.~~

~~Possession and control of an authenticator: The ability to activate and use the authenticator in an authentication protocol.~~

~~Practice Statement: A formal statement of the practices followed by the parties to an authentication process (i.e., RA, CSP, or verifier). It usually describes the policies and practices of the parties and can become legally binding.~~

~~Private Credentials: Credentials that cannot be disclosed by the CSP because the contents can be used to compromise the authenticator.~~

~~Private Key: The secret part of an asymmetric key pair that is used to digitally sign or decrypt data.~~

~~Protected Session: A session wherein messages between two participants are encrypted and integrity is protected using a set of shared secrets called session keys. A participant is said to be authenticated if, during the session, he, she or it proves possession of a long term authenticator in addition to the session keys, and if the other party can verify the identity associated with that authenticator. If both participants are authenticated, the protected session is said to be mutually authenticated.~~

~~Pseudonymous Identifier: A meaningless, but unique number that does not allow the RP to infer the subscriber but which does permit the RP to associate multiple interactions with the subscriber's claimed identity.~~

~~Public Credentials: Credentials that describe the binding in a way that does not compromise the authenticator.~~

~~Public Key: The public part of an asymmetric key pair that is used to verify signatures or encrypt data.~~

~~Public Key Certificate: A digital document issued and digitally signed by the private key of a Certificate authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. See also [RFC 5280].~~

~~Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.~~

~~Registration: The process through which an applicant applies to become a subscriber of a CSP and an RA validates the identity of the applicant on behalf of the CSP.~~

~~Registration Authority (RA): A trusted entity that establishes and vouches for the identity or attributes of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).~~

~~Relying Party (RP): An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.~~

~~Remote: (As in remote authentication or remote transaction) An information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls. Note: Any information exchange across the Internet is considered remote.~~

~~Replay Attack: An attack in which the attacker is able to replay previously captured messages (between a legitimate claimant and a verifier) to masquerade as that claimant to the verifier or vice versa.~~

~~Risk Assessment: The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.~~

~~Salt: A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.~~

~~Secondary Authenticator: A temporary secret, issued by the verifier to a successfully authenticated subscriber as part of an assertion protocol. This secret is subsequently used, by the subscriber, to authenticate to the RP. Examples of secondary authenticators include bearer assertions, assertion references, and Kerberos session keys.~~

~~Secure Sockets Layer (SSL): An authentication and security protocol widely implemented in browsers and web servers. SSL has been superseded by the newer Transport Layer Security (TLS) protocol; TLS 1.0 is effectively SSL version 3.1.~~

~~Security Assertion Mark-up Language (SAML): An XML-based security specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet.~~

~~SAML Authentication Assertion: A SAML assertion that conveys information from a verifier to an RP about a successful act of authentication that took place between the verifier and a subscriber.~~

~~Session Hijack Attack: An attack in which the attacker is able to insert himself or herself between a claimant and a verifier subsequent to a successful authentication exchange between the latter two parties. The attacker is able to pose as a subscriber to the verifier or vice versa to control session data exchange. Sessions between the claimant and the relying party can also be similarly compromised.~~

~~Shared Secret: A secret used in authentication that is known to the claimant and the verifier.~~

~~Social Engineering: The act of deceiving an individual into revealing sensitive information by associating with the individual to gain confidence and trust.~~

~~Special Publication (SP): A type of publication issued by NIST. Specifically, the Special Publication 800-series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.~~

~~Strongly Bound Credentials: Credentials that describe the binding between a user and authenticator in a tamper-evident fashion.~~

~~Subscriber: A party who has received a credential or authenticator from a CSP.~~

~~Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.~~

~~Token: See Authenticator.~~

~~Token Authenticator: See Authenticator Output.~~

~~Token Secret: See Authenticator Secret.~~

~~Transport Layer Security (TLS): An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by [RFC 5246]. TLS is similar to the older Secure Sockets Layer (SSL) protocol, and TLS 1.0 is effectively SSL version 3.1. NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations specifies how TLS is to be used in government applications.~~

~~Trust Anchor: A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate).~~

~~Trust Framework: In identity management, means a digital identity system with established identity, security, privacy, technology, and enforcement rules and policies adhered to by certified identity providers that are members of the identity trust framework. Members of an identity trust framework include identity trust framework operators and identity providers. Relying parties may be, but are not required to be, a member of an identity trust framework in order to accept an identity credential issued by a certified identity provider to verify an identity credential holder's identity. [§ 59.1-550, Code of Virginia]~~

~~Unverified Name: A subscriber name that is not verified as meaningful by identity proofing.~~

~~Valid: In reference to an ID, the quality of not being expired or revoked.~~

~~Verified Name: A subscriber name that has been verified by identity proofing.~~

~~Verifier: An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticator(s) and identity and check their status.~~

~~Verifier Impersonation Attack: A scenario where the attacker impersonates the verifier in an authentication protocol, usually to capture information that can be used to masquerade as a claimant to the real verifier.~~

~~Weakly Bound Credentials: Credentials that describe the binding between a user and authenticator in a manner than can be modified without invalidating the credential.~~

~~Zeroize: Overwrite a memory location with data consisting entirely of bits with the value zero so that the data is destroyed and not recoverable. This is often contrasted with deletion methods that merely destroy reference to data within a file system rather than the data itself.~~

~~Zero-knowledge Password Protocol: A password based authentication protocol that allows a claimant to authenticate to a Verifier without revealing the password to the verifier. Examples of such protocols are EKE, SPEKE and SRP.~~

2 Background

In 2015, the Virginia General Assembly passed the Electronic Identity Management Act (§§ 59.1-550 to -555) to address demand in the state's digital economy for secure, privacy enhancing digital authentication and identity management. Growing numbers of communities of interest have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – identity providers, credential service providers and relying parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in Appendix 1.

IMSAC recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an identity trust framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§§ 59.1-550 to -555); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Purpose Statement

This document outlines the Assurance Model established in the National Institute of Standards and Technology (NIST) Special Publication 800-63-3. The NIST Assurance Model serves as the primary reference for the concept of assurance in the context of digital authentication and identity management, and it serves as the basis for the types of assurance applied in the IMSAC guidance document series.

3 NIST Assurance Model

The minimum specifications developed by IMSAC, on behalf of the Secretary of Technology, use as a reference the Assurance Model documented in NIST SP 800-63-3. The minimum specifications assume that the identity trust framework for a digital identity system will define the specific assurance levels for that system, consistent with the NIST Assurance Model.[6] Therefore, the NIST ~~assurance model~~Assurance Model presented below should be viewed as a recommended framework for ~~electronic authentication~~digital authentication and identity management pursuant to the Electronic Identity Management Act.

Other ~~assurance model~~Assurance Models have been established in OMB M-04-04 and the State Identity, Credential, and Access Management (SICAM) guidelines, published by the National Association of State Chief Information Officers (NASCIO). A crosswalk showing disparities in the NIST SP 800-63-3, OMB M-04-04, and SICAM ~~assurance model~~Assurance Models has been provided in **Figure 1**.

Assurance Levels

~~T~~The NIST Assurance Model features two categories of assurance, relevant for the IMSAC guidance document series: Identity Assurance Level (IAL) and Authenticator Assurance Level (AAL). A third category of assurance in the NIST model, Federation Assurance Level (FAL), has been addressed in the *IMSAC Guidance Document: Federation and Participant Requirements*. The IALs and AALs are as follows:

Identity Assurance Level

Identity Assurance Level 1 – At this level, ~~attribute~~attributes provided in conjunction with the authentication process, if any, are self-asserted.

Identity Assurance Level 2 – IAL 2 introduces the need for either remote or in-person (physical or virtual) identity proofing. IAL 2 requires identifying attributes to have been verified in person or remotely using, at a minimum, the procedures given in NIST 800-63A.~~Identity Assurance Level 2 – IAL 2 introduces the need for either remote or in-person identity proofing. IAL 2 requires identifying attributes to have been verified in person or remotely using, at a minimum, the procedures given in NIST 800-63A.~~

Identity Assurance Level 3 – At IAL 3, in-person (physical or virtual) identity proofing is required. Identifying ~~attribute~~attributes must be verified by an authorized representative of the credential service provider (CSP) through examination of physical documentation as described in NIST 800-63A.

[6] ~~Trust Framework~~Identity Trust Frameworks for ~~identity management system~~Digital Identity Systems also should set requirements for how the assurance for each credential will be documented in the medata for the credential to support audit and compliance.

Authenticator Assurance Level

Authenticator Assurance Level 1 - AAL 1 provides single factor ~~electronic authentication~~digital authentication, giving some assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. AAL 1 allows a wide range of available authentication technologies to be employed and requires only a single authentication factor to be used. It also permits the use of any of the authentication methods of higher ~~authenticator~~authenticator assurance levels. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she possesses and controls the ~~authenticator~~authenticator.

A~~A~~uthenticator Assurance Level 2 – AAL 2 provides higher assurance that the same claimant who participated in previous transactions is accessing the protected transaction or data. Two different authentication factors are required. Various types of ~~authenticator~~authenticators, including multi-factor software cryptographic authenticators, may be used as described in NIST 800-63B. AAL 2 also permits any of the authentication methods of AAL 3. AAL 2 authentication requires cryptographic mechanisms that protect the primary ~~authenticator~~authenticator against compromise by the protocol threats for all threats at AAL 1 as well as verifier impersonation attacks. Approved cryptographic techniques are required for all ~~assertion~~assertion protocols used at AAL 2 and above.[7]

Authenticator Assurance Level 3 – AAL 3 is intended to provide the highest practical ~~electronic authentication~~digital authentication assurance. Authentication at AAL 3 is based on proof of possession of a key through a cryptographic protocol. AAL 3 is similar to AAL 2 except that only "hard" cryptographic ~~authenticator~~authenticators are allowed. The ~~authenticator~~authenticator is required to be a hardware cryptographic module validated at Federal Information Processing Standard (FIPS) 140 Level 2 or higher overall with at least FIPS 140 Level 3 physical security. AAL 3 ~~authenticator~~authenticator requirements can be met by using the PIV authentication key of a FIPS 201 compliant Personal Identity Verification (PIV) Card.

Figure 1. Assurance Model Crosswalk

OMB M04-04 Level of Assurance	SICAM Assurance Level	NIST SP 800-63-3 IAL	NIST SP 800-63-3 AAL
1	**1**	**1**	**1**
2	**2**	**2**	**2 or 3**

[7] Approved cryptographic techniques ~~shall~~must be FIPS approved, NIST recommended, or otherwise compliant with Commonwealth IT Information Security Standard (SEC501): http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/HostedEnvironmentInformationSecurityStandardSEC52501.pdf

3	**3**	**2**	**2 or 3**
4	**4**	**3**	**3**

577

578
579