NEW YORK STATE | Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Standard	**No:** NYS-S20-001
IT Standard: **Digital Identity**	**Updated:** 02/05/2025
	Issued By: NYS Office of Information Technology Services **Owner:** Chief Information Security Office

1.0 Purpose and Benefits

The purpose of this standard is to establish the rules and processes for maintaining and protecting New York State (NYS) identity data, including the tokens and credentials issued and bound to each identity.

The standard establishes a trustworthy process, based on National Institute of Standards and Technology (NIST) Digital Identity standards, for

- Identity proofing individuals.
- Managing authentication credentials that are tied to an individual's digital identity.
- Connecting that digital identity to the individual.

2.0 Authority

Section 103(10) of the State Technology Law provides ITS with the authority to establish statewide technology policies, including technology and security standards. Section 2 of Executive *Order No. 117*, established January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols, and standards for State government, including hardware, software, security, and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, *NYS-P08-002 Authority to Establish Enterprise Information Technology (IT) Policies, Standards and Guidelines.*

[1] All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021

3.0 Scope

This standard applies to all "State Entities" (SE), defined as "State Government" entities in Executive Order 117, established January 2002, or "State Agencies" as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any IT resource for which the SE or ITS has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE or ITS. While an SE may adopt a different standard, it must include the requirements set forth in this one. Where a conflict exists between this standard and an SE's standard, the more restrictive standard will take precedence. This standard is applicable to the authentication of all individuals or systems using or accessing NYS applications and systems for the purposes of conducting government business electronically. This includes all test, quality control, production and other ad hoc systems.

4.0 Information Statement

NYS has generally adopted the NIST 800-63-3: Digital Identity Guidelines, as the basis for electronic authentication standards where applicable and practical.

4.1 Enrollment and Identity Proofing

This section outlines the requirements for enrollment and identity proofing of applicants requesting access to IT resources at each Identity Assurance Level (IAL). The tables below reflect the Identity Assurance Levels determined by performing *the Identity Assurance Level Assessment Process* in Appendix B of the NYS-P20-001 Digital Identity Policy. Additionally, technical guidance from NIST 800-63A Digital Identity Guidelines: Enrollment and Identity Proofing is included in the tables below that will assist Credential Service Providers (CSP) and Information Owners in identifying and implementing the appropriate technical requirements.

IAL	Description
1	Low or no confidence in the asserted identity's validity
2	Confidence in the asserted identity's validity
3	High confidence in the asserted identity's validity

Identity Resolution - The CSP collects personally identifiable information (PII) from the person, such as name, address, date of birth, email, and phone number. See Appendix A for the different levels of strength for identity evidence (unacceptable, weak, fair, strong, superior), including the minimum requirements at each level, to establish a valid identity.	
IAL	**Standard**
1	Entered by applicant, self-asserted with no additional verification of identity information.
2	Applicant is uniquely identified, either in-person or unsupervised remote, through a managed registration process that includes, at a minimum, the following pieces of evidence: 1. Two pieces of strong evidence; OR 2. One piece of superior or strong evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of superior or strong evidence and the CSP validates the evidence directly with the issuing source; OR 3. One piece of strong evidence plus two pieces of fair evidence.
3	Applicant is uniquely identified, either in-person or supervised remote*, and verification through a managed registration process that includes, at a minimum, the following elements: 1. Two pieces of superior evidence; OR 2. One piece of superior evidence and one piece of strong evidence if the issuing source of the strong evidence, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of superior or strong evidence and the CSP validates the evidence directly with the issuing source; OR 3. Two pieces of strong evidence plus one piece of fair evidence.

***Per NIST SP 800-63A…**Supervised remote identity proofing is an equivalent approach to in-person proofing and requires a robust set of features. This includes high-resolution video monitoring through an agency-controlled device (e.g., not an applicant's personal phone), a trained operator on the other end of the video, and a number of other security controls. If those controls are all met, supervised remote identity proofing can achieve IAL3 (and IAL2).

Validation -- The CSP validates the information supplied in resolution by checking an authoritative source. The CSP determines the information supplied by the applicant matches their records.	
IAL	**Standard**
1	Information supplied by the applicant requires no validation by the CSP.

2	The CSP shall validate identity evidence as follows: Each piece of evidence must be validated with a process that can achieve the same strength as the evidence presented by the applicant. For example, if two forms of strong identity evidence are presented, each piece of evidence will be validated at a strength of strong.
3	The CSP shall validate identity evidence as follows: Each piece of evidence *must* be validated with a process that can achieve the same strength as the evidence presented by the applicant. For example, if two forms of strong identity evidence are presented, each piece of evidence will be validated at a strength of strong.

Verification - The CSP verifies the identity evidence provided by the applicant.	
IAL	**Standard**
1	Information supplied by the applicant requires no verification by the CSP.
2	The CSP shall verify identity evidence as follows: 1. At a minimum, the applicants binding to identity evidence must be verified by a process that is able to achieve a strength of strong. 2. Knowledge-Based Verification (KBV) shall not be used for in-person (physical or supervised remote) identity verification.
3	The CSP shall verify identity evidence as follows: 1. At a minimum, the applicants binding to identity evidence must be verified by a process that is able to achieve a strength of superior. 2. KBV shall not be used for in-person (physical or supervised remote) identity verification.

4.2 Authenticator Lifecycle Management

There are various events across the lifecycle of an authenticator that affect its use. Events include binding, loss, theft, damage, unauthorized duplication, expiration, revocation, and termination. The following tables will reflect the level of confidence at each Authenticator Assurance Level (AAL) that is achieved by performing the AAL Assessment Process in Appendix C in the NYS-P20-001 Digital Identity Policy. For additional implementation guidance, please see NIST 800-63Bsup1, Incorporating Syncable Authenticators into NIST SP-800-63B.

AAL	Description
1	Some assurance that the claimant controls an authenticator registered to the subscriber
2	High Confidence that the claimant controls an authenticator(s) registered to the subscriber
3	Very high confidence that the claimant controls an authenticator(s) registered to the subscriber

Authentication - Users assert their identity by presenting their credentials to a verifier to access an online service. Authenticator types must follow the requirements found in the NYS-S14-006 Authentication Tokens Standard, for their respective AAL levels.

AAL	Standard
1	Single-factor authentication, at a minimum
2	Multi-factor authentication, at a minimum
3	Multi-factor authentication using a hardware-based cryptographic authenticator and an authenticator that provides verifier-impersonation resistance. The same device may fulfill both these requirements.

Authenticator and Verifier Requirements - The verifier and CSP work together to ensure a token and its possessor's validity. All section references below refer to NIST SP 800-63B Authentication and Lifecycle Management.	
AAL	**Standard**
1	Cryptographic authenticators used at AAL1 shall use approved cryptography. Software-based authenticators that operate within the context of an operating system may, where applicable, attempt to detect compromise (e.g., by malware) of the user endpoint in which they are running and should not complete the operation when such a compromise is detected. Communication between the claimant and verifier (using the primary channel in the case of an out-of-band authenticator) shall be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to man-in-the-middle (MitM) attacks. Verifiers operated by government agencies at AAL1 shall be validated to meet the requirements of FIPS 140 Level 1.
2	Cryptographic authenticators used at AAL2 shall use approved cryptography. Authenticators procured by government agencies shall be validated to meet the requirements of FIPS 140 Level 1. Software-based authenticators that operate within the context of an operating system may, where applicable, attempt to detect compromise of the platform in which they are running (e.g., by malware) and should not complete the operation when such a compromise is detected. At least one authenticator used at AAL2 shall be replay resistant as described in Section 5.2.8. Authentication at AAL2 should demonstrate authentication intent from at least one authenticator as discussed in Section 5.2.9. Communication between the claimant and verifier (the primary channel in the case of an out-of-band authenticator) shall be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to MitM attacks. Verifiers operated by government agencies at AAL2 shall be validated to meet the requirements of FIPS 140 Level 1. When a device such as a smartphone is used in the authentication process, the unlocking of that device (typically done using a PIN or biometric) shall not be considered one of the authentication factors. Generally, it is not possible for a verifier to know that the device had been locked or if the unlock process met the requirements for the relevant authenticator type. When a biometric factor is used in authentication at AAL2, the performance requirements stated in Section 5.2.3 shall be met, and the verifier should make a determination that the biometric sensor and subsequent processing meet these requirements.

3	Communication between the claimant and verifier shall be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to MitM attacks. At least one cryptographic device authenticator used at AAL3 shall be verifier impersonation resistant as described in Section 5.2.5 and shall be replay resistant as described in Section 5.2.8. All authentication and reauthentication processes at AAL3 shall demonstrate authentication intent from at least one authenticator as described in Section 5.2.9. Multi-factor authenticators used at AAL3 shall be hardware cryptographic modules validated at FIPS 140 Level 2 or higher overall with at least FIPS 140 Level 3 physical security. Single-factor cryptographic devices used at AAL3 shall be validated at FIPS 140 Level 1 or higher overall with at least FIPS 140 Level 3 physical security. Verifiers operated by government agencies at AAL3 shall be validated at FIPS 140 Level 1 or higher. Verifiers at AAL3 shall be verifier compromise resistant as described in Section 5.2.7 with respect to at least one authentication factor. Hardware-based authenticators and verifiers at AAL3 should resist relevant side-channel (e.g., timing and power-consumption analysis) attacks. Relevant side-channel attacks shall be determined by a risk assessment performed by the CSP. When a device such as a smartphone is used in the authentication process — presuming that the device is able to meet the requirements above — the unlocking of that device shall not be considered to satisfy one of the authentication factors. This is because it is generally not possible for verifier to know that the device had been locked nor whether the unlock process met the requirements for the relevant authenticator type. When a biometric factor is used in authentication at AAL3, the verifier shall make a determination that the biometric sensor and subsequent processing meet the performance requirements stated in Section 5.2.3.

Renewal

The CSP should bind an updated authenticator an appropriate amount of time before an existing authenticator's expiration. The process for this should conform closely to the initial authenticator binding process (e.g., confirming address of record). Following successful use of the new authenticator, the CSP may revoke the authenticator that it is replacing.

Revocation and Termination

Revocation of an authenticator — sometimes referred to as termination, especially in the context of Personal Identity Verification (PIV) authenticators — refers to removal of the binding between an authenticator and a credential the CSP maintains.

CSPs shall revoke the binding of authenticators promptly when an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.

The CSP shall require subscribers to surrender or certify destruction of any physical authenticator containing certified attributes signed by the CSP as soon as practical after revocation or termination takes place. This is necessary to block the use of the authenticator's certified attributes in offline situations between revocation/termination and expiration of the certification.

Further requirements on the termination of PIV authenticators are found in FIPS 201.

Records Retention

The retention period is defined by applicable laws, regulations, or policies (e.g., New York State Archives General Retention Schedules). If the CSP opts to retain records in the absence of any mandatory requirements, the CSP shall conduct a risk management process that includes an assessment of the privacy and security risks, as defined in the NYS-S14-001 Information Security Risk Management Standard, to determine how long records should be retained. The user shall be informed of the retention policy.

Security Controls - The CSP implements and maintains appropriate security controls based on the assurance level. This Standard provides technical requirements for SEs implementing digital identity services and is not intended to constrain the development or use, outside of this purpose.	
AAL	**Standard**
1	Compliance with the NYS-P03-002 Information Security Policy is required. CSPs must employ appropriately tailored security controls from the *low* baseline of security controls defined in NIST 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. CSPs must ensure the minimum assurance requirements associated with this low baseline are satisfied. If there is a conflict between the two documents, the more restrictive document applies. An Information Security Exception Request must be filled out for those requirements that cannot be met, as outlined in NYS-P13-001 Information Security Exception Policy.
2	Compliance with the NYS-P03-002 Information Security Policy is required. CSPs must employ appropriately tailored security controls from the *moderate* baseline of security controls defined in NIST 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. CSPs must ensure the minimum assurance requirements associated with this moderate baseline are satisfied. If there is a conflict between the two documents, the more restrictive document applies. An Information Security Exception Request must be filled out for those

	requirements that cannot be met, as outlined in NYS-P13-001 Information Security Exception Policy.
3	Compliance with the NYS-P03-002 Information Security Policy is required. CSPs must employ appropriately tailored security controls from the *high* baseline of security controls defined in NIST 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. CSPs must ensure the minimum assurance requirements associated with this high baseline are satisfied. If there is a conflict between the two documents, the more restrictive document applies. An Information Security Exception Request must be filled out for those requirements that cannot be met, as outlined in NYS-P13-001 Information Security Exception Policy.

4.3 Federation and Assertions

Federation is a process that allows for the conveyance of authentication and subscriber attribute information across networked systems. In a federation scenario, the verifier or CSP is referred to as an identity provider, or IdP. The Relying Party (RP) is the party that receives and uses the information provided by the IdP. More information can be found in NYS-P20-001 Digital Identity Policy, and NIST SP 800-63C Federation and Assertions.

FAL	Description
1	Bearer assertion, signed by the IdP. The assertion being generated by the IdP shall meet a core set of requirements, including protection against modification or construction by an attacker by having the assertion contents signed by the IdP using approved cryptography. An RP shall verify the origin and integrity of the assertion upon receipt. All assertions shall be audience-restricted to a specific RP or set of RPs, and the RP shall validate that it is one of the targeted RPs for the given assertion. IdP shall ensure that any party holding the assertion, including the RP, is unable to impersonate the IdP at a non-targeted RP by protecting the assertion with a signature and key using approved cryptography. If the assertion is protected by a digital signature using an asymmetric key, the

	IdP may use the same public and private key pair to sign assertions to multiple RPs. If the assertion is protected by a keyed message authentication code (MAC) using a shared key, the IdP shall use a different shared key for each RP. The trust agreement between the IdP and RP may be established entirely dynamically, if not statically. For instance, the subscriber can identify their chosen IdP to the RP at runtime, allowing the RP to discover the IdP's parameters and register itself for use by the subscriber. The subscriber then, is prompted by the IdP to determine which attributes are released to the RP, and for what purposes.
2	Bearer assertion, signed by the IdP and encrypted to RP. All requirements at FAL1 apply at FAL2, except where overridden by more restrictive requirements. The assertion shall be strongly protected from being injected by an attacker. The assertion should be presented using back-channel presentation. In using back-channel presentation, the RP fetches the assertion directly from the IdP using a single-use assertion reference, preventing an attacker from injecting through an external access point. If front channel presentation is used, additional injection protections shall be implemented by the RP. Injection attacks can be further mitigated by always requiring that the federation transaction start at the RP instead of the IdP. The trust agreement between the IdP and RP shall be established statically, including establishing limits of which attributes are made available to the RP and for what purpose. The trust agreement may be bilateral between the IdP and RP or may be managed using a multilateral federation partnership. The registration may be dynamic, provided the RP and IdP can prove their connection at runtime to the established trust agreement. Proof can include presentation of software attestations and proof of control over URLs at trusted domains. Government-operated IdPs asserting authentication at FAL2 shall protect keys used for signing or encrypting those assertions with mechanisms validated at FIPS140 Level 1 or higher.

3	Holder of key assertion signed by the IdP and encrypted to RP. All requirements at FAL1 and FAL2 apply at FAL3, except where overridden by more restrictive requirements. The subscriber shall present a bound authenticator directly to the RP in addition to presenting an assertion. The bound authenticator need not be the same authenticator used by the subscriber to authenticate to the IdP. The assertion is used to identify the subscriber to the RP while the bound authenticator gives very high assurance that the party attempting to log in is the subscriber identified in the assertion. FAL3 is not reached at the RP until the subscriber authenticates with the bound authenticator and the RP verifies that the authenticator presented is correctly bound to the RP subscriber account identified by the assertion. The trust agreement and registration between the IdP and RP shall be established statically. All identifying key material and federation parameters for all parties shall be fixed before the federated authentication process can take place. Runtime decisions may be used to further limit what is sent between parties in the federated authentication process. IdPs asserting authentication at FAL3 shall protect keys used for signing or encrypting those assertions with mechanisms validated at FIPS140 Level 1 or higher.

5.0 Compliance

This standard shall take effect upon publication. Compliance is required with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, an SE shall request an exception through the Chief Information Security Office exception process.

6.0 Definitions of Key Terms

Except for terms defined in this standard, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

7.0 Contact Information

For assistance in interpretation, all inquiries, and requests for future enhancements can be submitted to the standard owner at:

Chief Information Security Office
Reference: NYS-S20-001
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: https://its.ny.gov/policies

8.0 Revision History

This policy should be reviewed consistent with the requirements set forth in ITS-P24-003 Process for Establishing Information Technology Polices, Standards and Guidelines.

Date	Description of Change	Reviewer
10/18/2013	Original Standard Release	Thomas Smith, Chief Information Security Officer
07/16/2020	Content updated to reflect NIST SP 800-63 revisions. Renamed standard from Identity Assurance (NYS-S13-004) to Digital Identity (NYS-S20-001).	Karen Sorady, Acting Chief Information Security Officer
05/20/2021	Updated Scope language	Karen Sorady, Acting Chief Information Security Officer
02/05/2025	Updated Scope language, Minor changes to reflect changes to Digital Identity Policy, Removal of Security Controls Standard, Update to current NIST 800-63 Guidelines	Chris DeSain, Chief Information Security Officer

9.0 Related Documents

NYS-P20-001 Digital Identity Policy

NYS-S14-006 Authentication Tokens Standard

NYS-S14-013 Account Management/Access Control

Standard NYS-S14-007 Encryption Standard

NIST Special Publication 800-63-3

NIST 800-83 r5 Security and Privacy Controls for Information Systems and Organizations

NIST 800-63Bsup1, Incorporating Syncable Authenticators into NIST SP-800-63B

Appendix A - STRENGTHS OF IDENTITY EVIDENCE

Strengths of Identity Evidence	
Strength	**Qualities of Identity Evidence**
Unacceptable	• Evidence validation was not performed, or validation of the evidence failed
Weak	• All personal details from the evidence have been confirmed as valid by comparison with information held or published by an authoritative source.
Fair	• Attributes contained in the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s), OR • The evidence has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, OR • The evidence has been confirmed as genuine by trained personnel, OR • The evidence has been confirmed as genuine by confirmation of the integrity of cryptographic security features.

Strong	• The evidence has been confirmed as genuine:
	  • using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, OR
	  • by trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified, OR
	  • by confirmation of the integrity of cryptographic security features.
	• All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

Superior	• The evidence has been confirmed as genuine by trained personnel and appropriate technologies including the integrity of any physical and cryptographic security features. • All personal details and evidence details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).