New York State Information Technology Standard	No: NYS-S20-001
IT Standard: Digital Identity	**Updated:** 07/16/2020
	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; and

- connecting that digital identity to the individual.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services (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 State Enterprise Information Technology (IT) Policy, Standards and Guidelines*.

3.0 Scope

This standard applies to all "State Entities" (SE), defined as "State Government" entities as defined 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 ITS resource for which ITS the SE has administrative responsibility, including systems managed or hosted by third parties on behalf of the ITS SE. While an SE may adopt a different standard, it must include the requirements set forth in this one.

This standard covers all systems developed by, or on behalf of, NYS that require authenticated access. This includes all test, quality control, production and other ad hoc systems.

This standard applies to the authentication of individuals of NYS applications and systems for the purposes of conducting government business electronically.

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 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 Registration Authorities (RA), 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 remotely, 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 requiring in-person appearance 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.

Validation - CSP validates the information supplied in registration by checking the 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 shall 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	Same requirements as IAL 2.

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.

Credential Issuance - CSP securely provides applicant's credential and any other required authentication tokens to the applicant.		
IAL	**Standard**	
1	Credentials are applicant defined (e.g., applicant chooses a user ID and password)	
2	*In-person:* If photo ID appears valid and the photo matches applicant: a) If personal information in records includes a telephone number or email address, the CSP issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or text message at the phone number or email address associated with the applicant in records. Any secret sent over an unprotected session shall be reset upon first use and will expire after 24 hours. User ID and token must be sent under separate cover; OR b) If ID confirms address of record, RA authorizes and CSP issues credentials in-person; OR c) If ID does not confirm address of record, RA confirms the applicant	*Remote:* a) CSP issues credentials in a manner that confirms the ability of the applicant to receive mail at a physical address associated with the applicant in records. Secrets sent must be reset on first use and will expire after 14 days. User ID and token must be sent under separate cover; OR b) If personal information in records includes a telephone number or e-mail address, the CSP issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or text message at the phone number or e-mail address associated with the applicant in records. Any secret sent over an unprotected session shall be reset upon first use and will expire after 24 hours. User ID and token must be sent under separate cover; OR c) If ID does not confirm address of record, RA confirms the applicant receives mail at

2	receives mail at the claimed address; then CSP issues credentials in-person.	the claimed address; then CSP issues credentials to the claimed address. RA or CSP sends notice to an address of record confirmed in the records check. Secrets sent must be reset on first use and will expire after 14 days. User ID and token must be sent under separate cover. Note: Agencies are encouraged to use methods a) and b) where possible to achieve better security. Method c) is especially weak when not used in combination with knowledge of account activity.
3	*In-person:* If photo ID appears valid and the photo matches applicant: a) If personal information in records includes a telephone number, the CSP issues credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records. Secrets sent shall be reset upon first use and will expire after 24 hours. User ID and token must be sent under separate cover; OR b) If ID confirms address of record, RA authorizes or CSP issues credentials in person; OR c) If ID does not confirm address of record, RA confirms the applicant receives mail at the claimed address; then CSP issues credentials in-person	*Remote:* a) CSP issues credentials in a manner that confirms the ability of the applicant to receive mail at a physical address associated with the applicant in records. Secrets sent must be reset on first use and will expire after 14 days. User ID and token must be sent under separate cover; OR b) If personal information in records includes both an electronic address and a physical address that are linked together with the applicant's name and are consistent with the information provided by the applicant, then the CSP may issue credentials in a manner that confirms the ability of the applicant to receive messages (SMS, Voice or e-mail) sent to the electronic address. Any secret sent over an unprotected session shall be reset upon first use and shall be valid for a maximum lifetime of 24 hours. User ID and token must be sent under separate cover.

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.

AAL	Description
1	Some assurance that the claimant controls an authenticator registered to the subscriber
2	Confidence that the claimant controls an authenticator(s) registered to the subscriber
3	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.	
AAL	**Standard**
1	Single-factor authentication Authenticator types must follow the requirements found in the NYS Authentication Tokens Standard for AAL1.
2	Multi-factor authentication Authenticator types must follow the requirements found in the NYS Authentication Tokens Standard for AAL2.
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 types must follow the requirements found in the NYS Authentication Tokens Standard for AAL3.

Credential Storage - CSP stores and protects the token and credentials from compromise at a level of security commensurate with the authenticator assurance level of the issued credential as per the NYS-S14-007 Encryption Standard.	
AAL	**Standard**
1	Passwords and shared secrets are protected using approved algorithms in accordance with the NYS-S14-007 ITS Encryption Standard. Access controls should also be implemented to limit access to administrators and other applications.
2	Passwords and shared secrets are protected using approved algorithms in accordance with the NYS-S14-007 ITS Encryption Standard. Access controls should also be implemented to limit access to administrators and other applications.
3	Passwords and shared secrets must be protected using a FIPS 140-2 Security Requirements for Cryptographic Modules, Security Level 2 or higher algorithm and should be protected by access controls limited to administrators and other applications.

	Token and Credential Verification Services - The verifier and CSP work together to ensure a token and its possessor's validity.
AAL	**Standard**
1	Long-term shared authentication secrets may be revealed to verifiers. If revealed, the secret must be changed upon next successful login.
	Assertions issued about claimants due to a successful authentication are cryptographically authenticated by the RP, using FIPS approved or NIST recommended methods, or are obtained directly from a trusted party via a secure authentication protocol.
2	Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the CSP; however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. If revealed, the secret must be changed upon next successful login.
	Cryptographic protections are required for all messages between the CSP and verifier.
	Assertions issued about claimants due to a successful authentication are either cryptographically authenticated by the RP, using FIPS approved or NIST recommended methods, or are obtained directly from a trusted party via a secure authentication protocol.
3	Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token and must first unlock the token with a password or biometric or must also use a password in a secure authentication protocol to establish two-factor authentication.
	Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the CSP, however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. If revealed, the secret must be changed upon next successful login.
	Cryptographic protections are required for all messages between the CSP and verifier. Assertions issued about claimants due to a successful authentication are either cryptographically authenticated by the RP, using approved methods, or are obtained directly from a trusted party via a secure authentication protocol.
	Verifiers and RPs will ensure that credentials are valid.

	Token and Credential Renewal/Re-issuance - The CSP establishes suitable policies for renewal and re-issuance of tokens and credentials.
AAL	**Standard**
1	Documented policy and procedures for renewal and re-issuance of unexpired tokens and credentials must be established by the CSP.
	Proof of possession of unexpired token to the CSP by the user is required.

	Passwords are only reissued, not renewed.
	Grace logons after expiration are allowed.
	Upon reissuance, token secrets shall not be set to defaults or reused in any manner.
	When issuing electronically, all interactions shall occur over protected sessions such as SSL/TLS.
2	In addition to Level 1 requirements:
	After expiration of current token and any grace period, renewal or reissuance is not allowed without the user re-establishing their identity with the CSP.
3	In addition to Level 2 requirements:
	Sensitive data transfers shall be cryptographically authenticated using keys bound to the authentication process.
	All temporary or short-term keys derived during the original authentication operation shall expire and re-authentication shall be required after not more than 24 hours from the initial authentication.

Token and Credential Revocation and Destruction - CSP revokes and maintains the revocation status and destroys credentials as needed.	
AAL	Standard
1	CSP establishes a process that allows for revocation of tokens and credentials within 72 hours after notification.
2	CSP establishes a process that allows for revocation of tokens and credentials within 24 hours after notification.
3	CSP establishes a process that allows for revocation of credentials within 24 hours after notification.
	Token destruction to occur within 48 hours.

Records Retention - The RA and the CSP maintain a record of the registration, history, and status of each token and credential.	
AAL	Standard
1	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 subscriber shall be informed of the retention policy.
2	The minimum record retention period for AAL2 credentials is seven years and six months beyond the expiration or revocation (whichever is later) of the credential unless

Records Retention - The RA and the CSP maintain a record of the registration, history, and status of each token and credential.	
AAL	**Standard**
	a longer timeframe is required by applicable laws, regulations, or policies (e.g., New York State Archives).A record of the registration, history, and status of each token and credential (including revocation) shall be maintained by the CSP or its representatives.
3	The minimum record retention period for AAL3 credential data is ten years and six months beyond the expiration or revocation of the credential unless a longer timeframe is required by applicable laws, regulations, or policies (e.g., New York State Archives). A record of the registration, history, and status of each token and credential (including revocation) shall be maintained by the CSP or its representatives.

Security Controls - The RA and the CSP implement and maintain appropriate security controls based on the assurance level.	
AAL	**Standard**
1	Compliance with the NYS-P03-002 Information Security Policy. CSP must employ appropriately tailored security controls from the <u>low</u> baseline of security controls defined in the NYS-S14-003 Information Security Controls Standard. CSP must ensure the minimum assurance requirements associated with this low baseline are satisfied. An Information Security Exception Request must be filled out for those requirements that cannot be met, as outlined in the Information Security Exception Policy. If there is a conflict between the two documents, the more restrictive applies.
2	Compliance with the NYS-P03-002 Information Security Policy. CSP must employ appropriately tailored security controls from the <u>moderate</u> baseline of security controls defined in the NYS-S14-003 Information Security Controls Standard. CSP must ensure the minimum assurance requirements associated with this moderate baseline are satisfied. An Information Security Exception Request must be filled out for those requirements that cannot be met, as outlined in the Information Security Exception Policy. If there is a conflict between the two documents, the more restrictive applies.
3	Compliance with the NYS-P03-002 Information Security Policy. CSP must employ appropriately tailored security controls from the <u>high</u> baseline of security controls defined in the NYS-S14-003 Information Security Controls Standard. CSP must ensure the minimum assurance requirements associated with this high baseline are satisfied. An Information Security Exception Request must be filled out for those requirements that cannot be met, as outlined in the Information Security Exception Policy. If there is a conflict between the two documents, the more restrictive applies.

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 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.

FAL	Description
1	Bearer assertion, signed by the IdP
2	Bearer assertion, signed by the IdP and encrypted to RP
3	Holder of key assertion signed by the IdP and encrypted to RP.

5.0 Compliance

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

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, 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.

Term	Definition
Knowledge-Based Verification (KBV)	Identity verification method based on knowledge of private information associated with the claimed identity. This is often referred to as knowledge-based authentication (KBA) or knowledge-based proofing (KBP).

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: http://www.its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
10/18/2013	Original Standard Release	Thomas Smith, Chief Information Security Officer
03/21/2014	Minor technical corrections in Token and Credential Renewal/Reissuance section; clarified rules for unprotected secrets in Credential Issuance section.	Thomas Smith, Chief Information Security Officer
09/19/2014	Minor wording changes to footnotes; added hyperlink for SICAM guidance and added to related documents	Deborah A. Snyder, Acting Chief Information Security Officer
03/10/2017	Updated Contact Information and Rebranding	Deborah A. Snyder, Deputy 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

9.0 Related Documents

[NYS-P10-006 Digital Identity Policy](#)

[NYS-S14-006 Authentication Tokens Standard](#)

[NYS-S14-013 Account Management/Access Control Standard](#)

[NYS-S14-007 Encryption Standard](#)

[NYS-S14-003 Information Security Controls Standard](#)

[NIST Special Publication 900-63-3](#)

Strengths of Identity Evidence	
Strength	**Qualities of Identity Evidence**
Unacceptable	No acceptable identity evidence provided.

Weak	• The issuing source of the evidence did not perform identity proofing.
	• The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the applicant.
	• The evidence contains:
	    ○ at least one reference number that uniquely identifies itself or the individual to whom it relates, OR
	    ○ a photograph or biometric template (of any type) of the individual.
	• Where the evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both. These methods ensure the integrity of the information and helps confirm the authenticity of the issuing source.

Fair	• The issuing source of the evidence confirmed the identity of an individual through an identity-proofing process.
	• The issuing process for the evidence means that it can be assumed to have been delivered to the correct individual.
	• The evidence:
	    ○ contains at least one reference number that uniquely identifies the person to whom it relates, OR
	    ○ contains a photograph or biometric template (any modality) of the person to whom it relates, OR
	    ○ can have ownership confirmed through Knowledge-Based Verification (KBV).
	• Where the evidence includes digital information, that information is protected using approved cryptographic or proprietary methods. These methods ensure the integrity of the information and helps confirm the authenticity of the claimed issuing source to be confirmed.
	• Where the evidence includes physical security features, it requires proprietary knowledge to be able to reproduce it.
	• The issued evidence is unexpired.

Strong	• The issuing source of the evidence confirmed the claimed identity through written procedures. Those procedures support a reasonable belief that the issuing source knows the real-life identity of the individual. Such procedures are subject to recurring oversight by regulatory or publicly accountable institutions. • The issuing process for the evidence ensured that it was delivered into the possession of the subject to whom it relates. • The issued evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the issued evidence must be the name that the individual was officially known by at the time of granting approval. Aliases, pseudonyms, or initials are not permitted.

Strengths of Identity Evidence	
Strength	**Qualities of Identity Evidence**
	• Where the evidence includes digital information, that information is protected using approved cryptographic and/or proprietary methods. Those methods ensure the integrity of the information and enable the authenticity of the issuing source. • The issued evidence is unexpired.
Superior	• The issuing source of the evidence confirmed the claimed identity by following written procedures that support a high confidence that the source knows the real-life identity of the individual. These procedures are subject to recurring oversight by regulatory or publicly accountable institutions. • The issuing source visually identified the applicant and performed further checks to confirm the existence of that person. • The issuing process for the evidence ensured that it was delivered into the possession of the person to whom it relates. • The evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the issued evidence must be the name that the individual was officially known by at the time of granting approval. Aliases, pseudonyms, or initials are not permitted. • The evidence contains a photograph of the individual. • The evidence contains a biometric template (of any type) of the individual. • Where the evidence includes digital information, that information is protected using approved cryptographic and/or proprietary methods. Those methods ensure the integrity of the information and enable the authenticity of the issuing source. • The evidence includes physical security features that require proprietary knowledge and technologies to be able to reproduce it. • The evidence is unexpired.