New York State Information Technology Standard	**No:** NYS-S14-006
IT Standard: **Authentication Tokens**	**Updated:** 12/01/2020
	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 list the appropriate authentication tokens that can be used with systems developed or operated for New York State (NYS) that require authenticated access depending on the Authenticator Assurance Level (AAL). This document also provides the requirements for management of those authentication devices.

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 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 applies to authentication of individuals accessing NYS information technology systems for the purposes of conducting government business electronically.

4.0 Information Statement

4.1   Assurance Levels and Required Token Types

The AAL of a system determines the degree of certainty required when authenticating a user. The following table describes the level of confidence associated with each AAL. These levels of assurance are consistent with those established by the US Federal Government for use by federal agencies.

Authenticator Assurance Level (AAL)	
AAL1	Provides some assurance that the claimant controls an "authenticator" bound to the subscriber's account. AAL1 requires either single-factor (e.g., password) or multi-factor (e.g., password + token) authentication using a wide range of available authentication technologies. Successful authentication requires that the individual logging in prove possession and control of the authenticator through a secure authentication protocol as defined in the NYS-S14-007 Encryption Standard.
AAL2	Provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors (multi-factor) is required through secure authentication protocol(s). Approved cryptographic techniques, as defined in the NYS-S14-007 Encryption Standard, are required at AAL2 and above.
AAL3	Provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication must use a hardware-based cryptographic authenticator and an authenticator that provides verifier impersonation resistance; the same device may fulfill both these requirements. To authenticate at AAL3, claimants must prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques as defined in the NYS-S14-007 Encryption Standard, are required at AAL3.

SEs must follow the Digital Identity Policy, NYS-P20-001 Digital Identity Policy, to determine the appropriate assurance level for their system. For token distribution requirements refer to the Digital Identity Standard, NYS-S20-001 Digital Identity Standard.

Each assurance level requires different authentication tokens which incorporate one or more authentication factors (i.e., something you know, something you have, and something you are). 1 requires a minimum of single factor authentication. AAL2 and 3 require multifactor authentication.

SEs must choose the appropriate token type(s) for their assurance level from Tables 1 or 2[1]. Table 1 shows the maximum assurance level that can be achieved with a single token type.

Table 1: Single-token Options

Token Types	AAL1	AAL2	AAL3
Memorized Secret	X		
Look-up Secret	X		
Out-of-Band Device	X		
Single-Factor One-Time Password Device (Hardware or Software)	X		
Single-Factor Cryptographic Hardware or Software	X		
Multi-Factor One-Time Password Device (Hardware or Software)		X	
Multi-Factor Cryptographic Software		X	
Multi-Factor Cryptographic Hardware Device			X

SEs may use multi-token authentication (i.e., a combination of tokens) to upgrade the overall level of assurance as depicted in Table 2.

---

[1] Token descriptions can be found in Section 4.2 – Authentication Token Types

Table 2: Multi-token Options

AAL2	AAL3		
AAL2 requires that a combination of single-factor authenticators must include a Memorized Secret token, and a possession-based second factor from the following list: • Look-up Secrets • Out-of-Band Device • Single-Factor One-Time Password (OTP) Device • Single-Factor Cryptographic Software • Single-Factor Cryptographic Device	AAL 3 requires the use of one of the following combination of authenticators:		
	Single-Factor Cryptographic Device	&	Memorized Secret
	Multi-factor OTP Device (hardware or software)	&	Single-Factor Cryptographic Device
	Multi-Factor OTP Device (hardware only)	&	Single-Factor Cryptographic Software Authenticator
	Single-Factor OTP Device (hardware only)	&	Multi-Factor Cryptographic Software Authenticator
	Single-Factor OTP Device (hardware only)	&	Single-Factor Cryptographic Software Authenticator **& Memorized Secret**
	Multi-Factor Cryptographic Hardware Device (Meets AAL3 with one device – See Table 1)		

4.2   Authentication Token Types

4.2.1 Memorized Secret Token

A memorized secret token is something you know. Memorized secret tokens are typically character or numerical strings. Examples include: passwords, passphrases, and Personal Identification Numbers (PINs).

Typically, a memorized secret token is used on its own for AAL1. AAL2 and 3 **require** multi-factor authentication (MFA). When a memorized secret token is used as one of the factors in a multi-factor authentication solution, the token requirements at the associated AAL apply.

The following table addresses the minimum requirements regarding memorized secret tokens. It is important to note that other requirements dictated by regulatory bodies (i.e., IRS for Federal Tax Information) may have different requirements. **An SE's relevant compliance domains should be consulted to address the authentication needs of a system.**

Table 3: Memorized Secret Token Minimum Requirements

Memorized Secret Management Standard	Description	Requirement
Password Length (Minimum)	The system enforced minimum number of characters required for an account password.	**PW Only Account**: 14 Characters – Encourage passphrase use **MFA Account**[2]: 8 Characters
Password Length (Maximum)	The system enforced maximum number of characters in a valid password	No limit, or maximum length allowed based on system constraints.
Password Composition	The system enforced character complexity of a valid password (allowing or disallowing certain characters types, or numbers of certain characters types).	Allow all character types in a password. **PW Only Account**: Require at least 1 non-alphabetical character. **MFA Account**: No composition requirement.
Password Expiration	The system enforced number of days that a password remains valid (forces a password change).	365 Days or upon indication of account compromise.
Password Banning	The system enforced check on new password creation against an internal deny list of known bad, weak, or recently used passwords.	Top 20 or more common bad passwords checked on new password creation. **Previously Used PW List**: Last 5 or more. **Password Change Delay**: 1 day or more.
Password Hints (Login)	The system allowing user defined password "hints" at login	Not allowed.

---

[2] This requirement applies to accounts that implement a password as part of a multifactor authentication solution. For example, an account that uses a soft/hard token one-time password device, combined with a PIN, would require an 8-character PIN/password.

Verifier Requirements

Where memorized secret tokens are randomly chosen by the Credential Service Provider (CSP) or verifier (i.e. onboarding with temporary password), tokens must be at least 6 characters in length and use an approved random bit generator.

Table 4 includes optional features that can enhance user experience.

Table 4: Memorized Secret Token Optional Recommendations

Memorized Secret Management Standard	Description	Recommendation
Password Strength Indicator	This is a feature (typically a 1 – 10 measurement) that shows the strength of a password.	Provide some form of password strength indication on creation.
Password Display	Allow display of the password the user is entering.	**On Creation**: Allow display of the entire password **On Entry**: Allow temporary display of each character as entered.
Password Manager	Use of external password management products	Encouraged especially in cases where users need to manage strong passwords for multiple accounts.
Copy/Paste	Allowing a cut/copied password to be pasted into a password field.	Only to facilitate a password management product usage.

4.2.2   Look-Up Secrets

A look-up secret is something you know, and a CSP/verifier has. It is either a physical or electronic record that stores a set of secrets shared between the user and CSP. An authenticator is used to look up the appropriate secret(s) needed to respond to a prompt from the verifier. An example is the use of a look-up secret as a "recovery key" for use when another authenticator is lost or malfunctions.

Look-up secrets are commonly used at AAL1. AAL2 and AAL3 require multifactor authentication. When combined with a memorized secret, the rules at AAL2 apply.

Authenticator Requirements – Look-up secrets must have at least 20 bits of entropy and must be distributed over a secure channel.

Table 5: Look-Up Secret Token (Shared Secret) Minimum Requirements

	Authenticator Assurance Levels		
	1	2[3]	3
Number of stored pre-registered knowledge tokens	7	MFA Required This token type cannot be used alone at these assurance levels without an CISO approved exception	
Number of correct pre-registered knowledge tokens user needs to provide	5		
Minimum number of characters	4		
Account locked after *x* number of consecutive failed attempts	5		
Allow words from shared secret questions to be used as the only word/phrase of the answer	No		
Allow the same shared secret answer for multiple questions	No		

4.2.3   Out-of-Band (OOB) Token

OOB tokens are something you have. They are a combination of a physical device (e.g., cellular phone, PDA, pager, land line) and a secret that is transmitted to the device over a distinct communications channel, by a verifier for one-time use.

An example of an OOB token would be a user logging into a website and receiving a text message or phone call on their cellular phone (pre-registered with the Credential Service Provider (CSP) during the registration phase) with a random authenticator to be presented as part of the electronic authentication protocol. E-mail cannot be used to transmit the random authenticator for the OOB device.

Authenticator Requirements - The device must be possessed and controlled by the user and uniquely addressable. The authenticator must establish a separate channel with the verifier to retrieve the out-of-band secret or authentication request. The secondary channel is considered out-of-band (even if it terminates on the same device) if the device does not leak information from one channel to the other without authorization from the claimant.

Use of the Public Switched Telephone Network (PSTN) is restricted unless the pre-registered telephone number in use is associated with a specific physical device. Changing the pre-registered telephone number is equivalent to the binding of a new authenticator and should follow applicable requirements. Voice Over Internet Protocol (VOIP) or email, must not be used for OOB authentication.

---

[3]When using a multi-factor solution for AAL2 or AAL3, as required, and one of the factors is a pre-registered knowledge token then AL2 standards apply.

Token Requirements - The token must be possessed and controlled by the user, uniquely addressable and must support communication over a channel/protocol that is separate from the primary channel/protocol for e-authentication.

Uniquely addressable means that the token can be addressed by a unique characteristic (e.g., phone number).

When accessing an application via a mobile device and using a virtual phone and communications management system (i.e., Google Voice), then that mobile device will not be viable as an OOB token as there is no separate channel/protocol for communication of the random authenticator.

A limitation with the use of OOB tokens is that if the device is infected, even if the communication occurs over a separate channel/protocol, both forms of authentication (application access and receipt of token) are compromised and all communication is therefore un-trusted.

Verifier Requirements – The maximum time-period that an OOB token can exist is 10 minutes and it can only be used once. The verifier-generated secret must have at a minimum 20 bits of entropy, however any authentication secret that has less than 64 bits of entropy must limit the number of failed authentication attempts to no more than 100.

4.2.4 Single Factor (SF) Cryptographic Device

SF cryptographic devices are something you have. It is a hardware device that performs cryptographic operations on input provided to the device. It does not require a second factor. Generally, it is a signed message. An example would be a Secure Socket Layer/Transport Layer Services (SSL/TLS) certificate.

Authenticator Requirements – The cryptographic modules used shall be validated at FIPS 140-2, Level 1 or higher. Products validated under subsequent versions of FIPS 140 are also acceptable.

Verifier Requirements – The input (e.g., a nonce or challenge) to generate the token has at least 64 bits of entropy and shall either be unique over the authenticator's lifetime, or statistically unique using an approved random bit generator. Verification must use approved cryptography.

4.2.5 Single-Factor (SF) One-Time Password (OTP) Device

SF OTP devices are something you have. This category includes hardware devices and software-based OTP generators installed on devices such as mobile phones. . This device has an embedded secret that is used as the seed for generation of OTPs and does not require activation through a second factor. Authentication is accomplished by providing an acceptable OTP and thereby proving user possession and control of the device. The device is used each time authentication is required.

Examples include key fob tokens, or software-based OTP generator. A user attempts to log into a website and provides a token generated code or OTP.

Authenticator Requirements – An approved block cipher or hash function to combine a symmetric key stored on the device with a nonce to generate an OTP must be used. The nonce may be a date and time or a counter generated on the device.

Verifier Requirements - The OTP shall have a limited lifetime, with a maximum of 2 minutes. The cryptographic module performing the verifier functions shall be validated at FIPS 140-2 Level 1 or higher. Products validated under subsequent versions of FIPS 140 are also acceptable.

4.2.6 Multi-Factor (MF) Software Cryptographic Token

A MF software cryptographic token is something you have, and it must be unlocked by either something you know or something you are. It is a cryptographic key that is stored on a disk or some other "soft" media and must be unlocked through a second factor of authentication separate from the authentication factor used to access the disk or other "soft" media.

Authentication is accomplished by proving possession and control of the key. The token is highly dependent on the specific cryptographic protocol, but it is generally some type of signed message.

An example would be a private cryptographic certificate that is unlocked by a passphrase that is separate from that which unlocks the device on which the certificate is stored. The certificate deployed on the user's workstation (something you have) in combination with a passphrase (something you know) provides multi-factor authentication. The password to access the device cannot automatically unlock the certificate.

Authenticator Requirements - The cryptographic module shall be validated at FIPS 140-3 Level 1 or higher. Products validated under subsequent versions of FIPS 140 are also acceptable. Each authentication shall require entry of the password or other activation data and the unencrypted copy of the authentication key shall be erased after each authentication.

Verifier Requirements – Verifier generated token input (e.g., a nonce or challenge) has at least 64 bits of entropy.

4.2.7 Multi-Factor (MF) One-Time Password (OTP) Device

A MF OTP device is something you have, and it must be unlocked by either something you know or something you are. It is a hardware and software-based device that generates OTPs for use in authentication and which must be unlocked through a second factor of authentication. The second factor of authentication may be achieved through an integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port).

The OTP is typically displayed on the device and manually input to the verifier as a password, although direct electronic input from the device to a computer is also allowed.

An example would be a key fob token in combination with a PIN. A user attempts to log into a website and provides a user-defined PIN (established when the token was assigned) and a token generated code. The combination of the PIN and token generated code is referred to as a passcode.

Authenticator Requirements - The cryptographic module shall be validated at FIPS 140-2 Level 2 or higher with the token itself meeting physical security at FIPS 140-2 Level 3 or higher. This means the token is tamper proof; it can't be broken open to reverse engineer or get a seed value, etc. Products validated under subsequent versions of FIPS 140 are also acceptable. Refer to the NYS-S14-007 Encryption Standard for additional information.

The OTP must be generated using an approved block cipher or hash function to combine a symmetric key stored on a personal hardware device with a nonce to generate an OTP. The nonce may be a date and time or a counter generated on the device. Each authentication shall require entry of a password or other activation data through an integrated input mechanism.

Verifier Requirements - The OTP shall have a limited lifetime, with a maximum of 2 minutes.

4.2.8 Multi-Factor (MF) Cryptographic Device

A MF cryptographic device is something you have, and it must be unlocked by either something you know or something you are. It is a hardware device that contains a protected cryptographic key that must be unlocked through a second authentication factor.

Authentication is accomplished by proving possession of the device and control of the key. The token is highly dependent on the specific cryptographic device and protocol, but it is generally some type of signed message. For example, in Transport Layer Services (TLS), there is a "certificate verify" message. An example would be an ATM card.

Authenticator Requirements - Cryptographic module shall be FIPS 140-2 validated, Level 2 or higher; with the token itself meeting physical security at FIPS 140-2 Level 3 or higher. This means the token is tamper proof; it can't be broken open to reverse engineer or get a seed value, etc. Products validated under subsequent versions of FIPS 140 are also acceptable.

Entry of a password, PIN, or biometric is required to activate the authentication key. The export of authentication keys is not allowed.

Verifier Requirements – Verifier generated token input (e.g., a nonce or challenge) has at least 64 bits of entropy.

4.3   Token Renewal/Re-issuance

Some token types support the process of renewal, while some support re-issuance. Depending on the assurance level, the user will need to re-establish their identity with the CSP if the token has expired or prove possession of the unexpired token before renewal or re-issuance occurs. Refer to the NYS-S20-001 Digital Identity Standard for additional information.

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 standard is necessary to support a business function, SEs 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
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 token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier.
Authentication Factors	Something you know, something you have, and something you are.
Credential Service Provider (CSP)	A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers.
Authenticator	Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity (e.g. token).
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.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Office
Reference: NYS-S14-006
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
03/21/2014	Original Standard Release; replaces *CSCIC/OCS User Password Management Standard (S10-004)* and *CSCIC/OCS Privileged Accounts Management Standard (S10-003)*	Thomas Smith, Chief Information Security Officer
08/15/2014	Added row to Table 3: Memorized Secret Token Requirements to require temporary passwords be changed on first logon	Deborah A. Snyder, Acting Chief Information Security Officer
03/20/2015	Changed password management and composition standards in Table 3	Deborah A. Snyder, Deputy Chief Information Security Officer
05/15/2015	Clarification to token renewal/re-issuance.	Deborah A. Snyder, Deputy Chief Information Security Officer
02/15/2017	Update to Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
07/16/2020	Update revised Scope and Authority and update links from Identity Assurance to Digital Identity	Karen Sorady, Acting Chief Information Security Officer

12/1/2020	Update to align industry best practices and federal guidelines	Karen Sorady, Chief Information Security Officer
01/21/2021	Table 3 Requirement wording updated	Karen Sorady, Chief Information Security Officer
05/19/2021	Updated Scope language	Karen Sorady, Chief Information Security Officer

9.0 Related Documents

NYS-P10-006 Digital Identity Policy

NYS-S13-004 Digital Identity Standard

NIST 800-63 Digital Identity Guidelines

NYS-S14-007 Encryption Standard