Queens College **Technology Standard**	**No: QC-ITS-Cyber-007**
Authentication Tokens	**Updated: 08/21/2023**
	Issued By: Queens College, Office of Chief Information Security Officer **Owner: Queens College Information Technology Services**

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 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

- **Responsible Office(s):** Queens College Information Technology Services
- **Responsible Executive(s)**: Chief Information Officer (CIO)
- **Responsible Officer(s)**: Chief Information Security Officer (CISO)

3.0 Scope: College Wide

This is a college-wide standard and includes requirements that must be followed if Queens College is to protect the information that is collected in the standard process of business. This standard is to be an additional layer of security on top of existing CUNY security policies and is not intended or able to supersede CUNY policies.

This standard encompasses all systems, automated and manual, for which Queens College has administrative responsibility, including systems managed or hosted by third parties on behalf of Queens College. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

4.0 Information Statement

4.1 Assurance Levels and Required Token Types

The Authenticator Assurance Level (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 U.S. Federal Government for use by federal agencies[1].

Authenticator Assurance Level (AAL)	
AAL1	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 Encryption Standard.
AAL2	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 Encryption Standard are required at AAL2 and above.
AAL3	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 are required.

[1] Described in NIST Special Publication 800-63-3–Digital Identity Guidelines

The entity must identify the appropriate assurance level for their system. 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). Authenticator Assurance Levels (AAL) 1 and 2 require single factor authentication. AAL 3 requires multifactor authentication.

Entities must choose the appropriate token type(s) for their assurance level from Tables 1 or 2. 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 Token	X		
Look-up Secrets Token	X		
Out of Band Token	X		
Single-Factor One-Time Password Device	X		
Single-Factor Cryptographic Device	X		
Multi-factor Software Cryptographic Device		X	
Multi-Factor One-Time Password Hardware Device		X	
Multi-Factor Hardware Cryptographic Device			X

Entities may use multi-token authentication (i.e., a combination of tokens) to upgrade the overall level of assurance as depicted in Table 2. For example, AAL3 can be achieved using two tokens rated at AAL2 that represent two different authentication factors (i.e., something you know, something you have, and something you are).

Table 2: Multi-token Options

<table>
<tr><th>AAL 2</th><th colspan="2">AAL 3</th></tr>
<tr><td rowspan="5">AAL 2 requires that a combination of single-factor authenticators must include a Memorized Secret authenticator, and a second factor that is possession-based from the following list:
• Look-up Secrets
• Out-of-Band Device
• Single-Factor OTP Device
• Single-Factor Cryptographic Software
• Single-Factor Cryptographic Device</td><td colspan="2">AAL 3 requires the use of one of the following combination of authenticators:</td></tr>
<tr><td>1. Memorized Secret</td><td>• Single-Factor Cryptographic Device</td></tr>
<tr><td>2. Multi-Factor OTP device (software and hardware)</td><td>• Single-Factor Cryptographic Device</td></tr>
<tr><td>3. Single-Factor OPT device (hardware only)</td><td>• Multi-Factor Cryptographic Software Authenticator</td></tr>
<tr><td>4. Single-Factor OTP device (hardware only)</td><td>• Single-Factor Cryptographic Software Authenticator
• Memorized Secret</td></tr>
</table>

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 AAL 1. AAL 2 and 3 **requires** multi-factor authentication. 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 base minimum requirements regarding Memorized Secret Tokens. Other compliance requirements may require stricter minimum requirements. Relevant compliance domains should be consulted to address specific systems, applications, etc.

Table 3: Memorized Secret Token Minimum Requirements

	Assurance Levels		
Category	**1**	**2[2]**	**3**
Password Management Standards			
Password expiration after *x* days	731	183	Multi Factor Authentication Required This token type can only be used with select authenticators at AAL 2 and 3. Refer to Table 2 for more information.
System to provide password expiration messages starting at least *x* days before expiration	14		
Password reuse	After 24 unique passwords		
Minimum password age	2 days		
Maximum number of grace logons after expiration, to allow for password change	1		
Temporary passwords changed immediately on first logon	Yes		
Password Composition Standards[3]			
Password must not be the same as the user ID	Yes		Multi Factor Authentication Required This token type can only be used with select authenticators at AAL 2 and 3. Refer to Table 2 for more information.
Minimum length	8		
Maximum number of repeating characters	3		
Minimum number of upper-case letters	1		
Minimum number of lower-case letters	1		
Minimum number of letters	3		
Minimum number of digits	1 or Symbol		
Minimum number of special characters	1 or Digit		

4.2.2 Look-Up Secrets

A look-up secret is something you have. It is either a physical or electronic record that stores a set of secrets shared between the user and CSP. The 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 AAL 1. AAL 2 and 3 require multifactor authentication. When combined with a memorized secret, the rules at AAL 2 apply.

[2] When using a multi-factor solution for AAL2 and AAL3, as required, and one of the factors is a memorized secret, then AAL2 standards apply.

[3] It is acknowledged that not all systems will be able to enforce all of these standards. In those cases, an exception request may be sought from the Chief Information Security Officer (CISO).

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

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.

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 and 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. It is a hardware device that supports the spontaneous generation of OTPs. 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. 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 140-2 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 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 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

All tokens must expire within two years of issuance. A warning notification of token expiration must be provided to the user within a minimum of 14 days of expiration.

Once the token has expired, it will be automatically disabled and/or locked from use.

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.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended 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, entities shall request an exception through the Chief Information Security Officer's exception process.

6.0 Definitions of Key Terms

Term	Definition

7.0 Contact Information

Submit all inquiries and requests for future enhancements to:

Chief Information Security Officer
Damon Vogel
CISO@qc.cuny.edu

8.0 Revision History

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

Date	**Description of Change**	**Reviewer**
9/20/22	Initial changes to apply to Queens College	DVogel
06/12/2023	Added Policy # & Tags	DVogel
08/21/2023	Conversion to Standard, Add #10, Alignment to Gartner Recommendations	DVogel

9.0 Related Documents

Encryption Standard

10.0 External Documents

NIST 800-63 Digital Identity Guidelines