Standards and Guidance for Authentication of External Users

July 22, 2021
Version 1.0

Revision History

Date	Action	Notes	Approved by
7/22/2021	Initial Version		Chip Stewart

Introduction

As government services transition to online delivery, validation of citizen's digital identities is an important component of protecting the confidentiality and integrity of the data we manage. The predominant mechanism for proofing a digital identity assertion is digital authentication. The digital authentication process validates one or more authenticators, which are commonly categorized as:

- Something you know (e.g., a memorized secret, such as a password)
- Something you have (e.g., a hardware token)
- Something you are (e.g., a biometric authenticator, such as a fingerprint)

The State is working towards a Single Sign-On (SSO) identity for each citizen that will allow for Authentication Assurance Levels (AAL) commensurate with the sensitivity of the data that is being accessed or provided (Contextual authentication). Until that occurs, the State is obligated to utilize other tools to provide adequate protection against unauthorized access to systems and information. This protection may include the use of Multi-Factor Authentication (MFA) to gain further assurance of the digital identity.

This Guidance is issued to clarify the standards applicable for authentication of identity assertions and provide guidance in selecting appropriate controls. This Guidance does not provide standards or intend to offer guidance for proofing a digital identity. The information within this Guidance is non-exhaustive.

Key Takeaways

- The authentication standards described in the Maryland IT Security manual are focused on security configurations for the operations and maintenance of a system.
- This document is meant to provide guidance regarding end-user configurations and requirements.
- Units must develop a standard for each citizen-facing application that provides reasonable security based on the sensitivity of the system, while facilitating a good customer experience.
- The guidance from NIST SP 800-63B should be used to set authentication requirements.
- MFA, when practical, should be used.
- MFA should support at least one Non-Visual Access compliant authentication mechanism.
- Systems should use tools to identify compromised passwords, either on account creation or continuously, to minimize the likelihood of common attacks that result in unauthorized account access.
- Users should be forced to re-authenticate before using sensitive features, such as changing authentication details.

Background

Recently, the National Institute of Standards and Technology (NIST) released updated guidance on the best practices related to Memorized Secrets. Memorized Secrets is a catch-all term that describes passwords, pass-phrases, and numeric character strings. Much of what has been developed recently, as referenced below, conflicts with the best practices that preceded the release of these documents. Many of the outdated security practices, such as those described below, reduce the security and encourage undesirable behavior, instead of improving security. These practices include:

- Time-based password expiration (e.g., passwords expire after 45 days)
- Unnecessary complexity requirements
- Unreasonably limiting the number of characters in the password
- Unreasonably limiting the type of characters in the password
- Prohibiting pasting into a password field or auto-filling passwords

Passwords are the most common type of memorized secret authenticator, and facilitate an easy user interaction. While typically called a second-factor, authenticators may also be:

- Out-of-Band device or service (OOB),
- One-Time-Password device, with or without multi-factor (OTP)
- Cryptographic Software Authenticators, with or without multi-factor (CSA)
- Cryptographic Device Authenticators, with or without multi-factor (CDA)

These authentication factors provide the verifier, such as a State web application, with an assurance that the requestor owns the digital identity. When combined, they provide a stronger level of assurance that the requestor is truly the owner of the digital identity. There are three Authentication Assurance Levels (AAL) described in the NIST SP 800-63B document that represent increasing levels of assurance:

- AAL1 - provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or multi-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.
- 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 is required through secure authentication protocol(s). Approved cryptographic techniques 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 SHALL use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance — the same device MAY fulfill both of these requirements. In order to authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.

Standards and Guidance

The standards and guidance below describe the creation, storage, transmission, and recovery of authenticators.

Creating Memorized Secrets

As part of creating and maintaining a digital identity, users must establish a memorized secret. Additionally, as part of normal system use, users may choose to change their password. Each unit or system owner must establish and enforce a standard for memorized secrets based on the criteria below. The standard should consider both the sensitivity of the system and the totality of the authentication transaction. At a minimum, systems:

must:

- Require re-authentication when memorized secrets or other authenticators are changed.
- Enforce a minimum length of no fewer than 12 characters.
- Allow a maximum length of at least 64 characters.
- Allow usage of all characters including unicode and whitespace.
- Process the characters exactly as entered.

must not:

- Silently truncate passwords on creation or entry.
- Provide password hints or allow for other knowledge-based authentication.

should:

- Validate the proposed memorized secret to ensure that it does not appear in dictionaries and corpuses of breached passwords.
    - Attempts to use a password from one of these lists should be rejected.
- Provide the user, at their option, the ability to see their proposed password while typing.
- Implement a password strength meter.
- If a password generator is not available, written guidance should be provided as to how to establish a strong password.
- If a system emails or texts an assigned password to users, force users to reset passwords upon initial sign in.

Storage and Processing of Authenticators

Units must ensure that systems store and process authenticators securely. This includes ensuring that multiple layers of protection are employed.

Units must:

- Utilize one of the following mechanisms to store passwords, in order of preference:
    - PBKDF2 with a work factor greater than 310,000 and set with an internal hash function of HMAC-SHA-256
    - Argon2id with a minimum configuration of 15MiB of memory, an iteration count of 2, and 1 degree of parallelism.
    - BCrypt with a work factor of 10 or more and with a password length limit of 64 characters.
- Prohibit transmission of authenticators on unencrypted channels.

Units Should

- Consider the use of a pepper, in addition to the salting provided by the hashing algorithm.
- Ensure that passwords are never sent in clear-text by hashing or encrypting outside of the communications channel.

Units should not:

- Force users to change their passwords in a pre-set time period (e.g., every 90 days);
- Require PII as a way to authenticate users;

- Provide a temporary password; if that cannot be avoided enforce an immediate password change upon initial sign in.

Authenticator Verification

When a requester attempts to login, the system must ensure that the transaction is protected from eavesdropping by using strong encryption across untrusted networks.

The system must:

- Provide a login landing page using TLS or a comparable security protocol.
- Implement a mechanism that makes brute-force attacks and bot-based login attempts infeasible.
- Support at least one Non-Visual Access compliant authentication mechanism.

The system should:

- allow, at the user's discretion, the ability to see the password entered.
- allow the user to paste their password into the password field.
- check password against blacklists on creation, and entry, if possible.
- remember the web browser to limit re-authentication with a second factor.
- implement a tool that compares passwords to a blacklist or to known compromised passwords. If passwords can be compared to a blacklist upon entry, this should be preferred;
- rather than lock a user out, institute a delay for retrying (e.g., wait 1 minute and try again)

The system must not:

- allow password hints or recovery methods that are knowledge-based
- allow for a denial of service circumstance to be created through an attacker (e.g., brute force account lock-outs)
-

Account Recovery and and Authenticator Resets

Users will inevitably forget or lose one or more of their authenticators and need to recover access to their account. The design of the system should consider this eventuality and facilitate easy account recovery. The goal of the recovery process is to allow the system (verifier) to ensure that the recovery requester (requester) is the owner of the digital identity. In cases where the lost authenticator is a memorized secret, the account recovery process should end with a reset of the memorized secret.

Because recovery actions create an opportunity for an unauthorized individual to take control of a digital identity, the process must ensure that appropriate controls are in place to prevent this. These controls should also permit the owner of the digital identity to recover access in the event that authenticators are lost. Therefore, systems:

must:

- provide a mechanism for account recovery that can occur completely out-of-band (e.g., in-person) if the loss of an identity would result in a financial loss or the permanent loss of personal data.

- Notify the owner of the identity when account recovery actions occur
- return a consistent message, in consistent time, whether or not the account exists

should:

- employ mechanisms to prevent or reduce automated recovery attempts
- use out-of-band communication such as email or text, where possible, to further validate the authenticity of the request
- Use expiring reset links instead of temporary passwords, and limit the duration of link to a reasonable duration
- consider the use of static Look-Up Secrets (e.g., backup codes) as a digital identity verifier
- consider supporting the use of a backup email or phone number in the event that the primary email or phone number is no longer available
- logout any existing sessions following a successful recovery

should not:

- use information that is publicly available
- use information that is frequently shared (e.g., online quizzes)
- use Personal Information/Personally Identifiable Information (PII) OR Protected Health Information (PHI) as the sole arbiter in an account recovery process

For more information on securely resetting passwords, please refer to the OWASP Forgot Password Cheat Sheet.

Definitions

1. **Authenticator Assurance Level (AAL) -** A category describing the strength of the authentication process.
2. **Memorized Secret -** A type of authenticator consisting of a character string intended to be memorized or memorable by the subscriber, permitting the subscriber to demonstrate something they know as part of an authentication process.
3. **Multi-Factor Authentication (MFA)** - An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. (The three authentication factors are something you know, something you have, and something you are).
4. **MUST** - This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
5. **MUST NOT** This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
6. **SHOULD** This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
7. **SHOULD NOT** This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

8. **MAY** This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)