Microsoft

Achieving National Institute of Standards and Technology Authenticator Assurance Levels with the Microsoft Identity Platform

About this paper

This whitepaper details methods for Achieving National Institute of Standards and Technology (NIST) Authenticator Assurance Levels (AALs) using the Microsoft Identity Platform. These standards are found in NIST Special Publication 800-63B: Authentication and Lifecycle Management.

It is intended for architects and other decision makers who want to determine the appropriate AAL for their organization and provides guidance on how to achieve the chosen level. AALs are one part of the overall NIST Special Publication 800-63: Digital Identity Guidelines. We encourage you to consume the overall NIST guidelines to understand how AALs fit in.

Please always check for the latest version of this document at https://aka.ms/Microsoft-NIST-AAL.

Contents

Why pursue NIST Digital Identity Guidelines?

The National Institute of Standards and Technology (NIST) develops the technical requirements for US federal agencies implementing identity solutions. Meeting these requirements is also required for organizations working with federal agencies. The NIST Identity requirements are found in the document Special Publication 800-63 Revision 3 (NIST SP 800-63-3).

NIST SP 800-63 is also referenced by the Electronic Prescription of Controlled Substances (ECPS) program and used in the Financial Industry Regulatory Authority Financial Industry Regulatory Authority (FINRA) requirements. Healthcare, defense, and other industry associations often use the NIST SP 800-63-3 as a baseline for identity and access management (IAM) requirements.

NIST guidelines are leveraged and referenced in other standards, most notably the Federal Risk and Authorization Management Program (FedRAMP) for Cloud Service Providers (CSPs). Azure is FedRAMP High certified, in addition to meeting 90+ other compliance offerings. See Trust your cloud for details on Azure compliance and certifications.

The NIST digital identity guidelines cover proofing and authentication of users such as employees, partners, suppliers, and customers or citizens.

The NIST SP 800-63-3 digital identity guidelines encompass three areas:

- SP 800-63A covers Enrollment & Identity Proofing
- SP 800-63B covers Authentication & Lifecycle management
- SP 800-63C covers Federation & Assertions

Each area has mapped out assurance levels. **This paper provides guidance for attaining the Authenticator Assurance Levels (AALs) in NIST SP 800-63B by using the Microsoft Identity Platform and other Microsoft solutions.**

About Authenticator Assurance Levels

NIST SP 800-63B defines the technical guidelines for the implementation of digital authentication. It does so with a framework of Authenticator Assurance Levels (AALs). AALs characterize the strength of the authentication of a digital identity. The guidance also covers management of the lifecycle of authenticators including revocation.

The standard denotes requirements for each AAL in terms of 11 requirement categories:

- Permitted authenticator types
- Federal Information Processing Standards 140 (FIPS 140) verification level (FIPS 140 requirements are satisfied by FIPS 140-2 or newer revisions)
- Reauthentication
- Security controls
- Man-in-the-middle (MitM) resistance
- Verifier-impersonation resistance (phishing resistance)
- Verifier-compromise resistance
- Replay resistance
- Authentication intent
- Records Retention Policy
- Privacy Controls

Applying NIST AALs in your environment

We recommend that you meet at least AAL 2, unless business reasons, industry standards, or compliance requirements dictate that you meet AAL3.

In general, AAL1 is not recommended because it accepts password-only solutions, and passwords are the most easily compromised form of authentication. See Your Pa$$word doesn't matter.

While NIST does not require verifier impersonation (AKA credential phishing) resistance until AAL3, we highly advise you address this threat at all levels. You can do this by selecting authenticators that provide verifier impersonation resistance, such as requiring Azure AD joined or hybrid Azure AD joined devices. If you are using Office 365 you can address this by using Office 365 Advanced Threat Protection, and specifically Anti-phishing policies.

As you evaluate the appropriate NIST AAL for your organization, you can consider whether your entire organization must meet NIST standards, or if there are specific groups of users and resources that can be segregated, and the NIST AAL configurations applied to only a specific group of users and resources.

Security controls, privacy controls, records retention policy

Azure and Azure Government have earned a Provisional Authority to Operate (P-ATO) at the NIST SP 800-53 High Impact Level from the Joint Authorization Board, the highest bar for FedRAMP accreditation, which authorizes the use of Azure and Azure Government to process highly sensitive data.

These Azure and Azure Government certifications satisfy the security controls, privacy controls and records retention policy requirements for AAL1, AAL2 and AAL3.

The FedRAMP audit of Azure and Azure Government included the information security management system that encompasses infrastructure, development, operations, management, and support of in-scope services. Once a P-ATO is granted, a Cloud service provider still requires an authorization (an ATO) from any government agency it works with. For Azure, a government agency, or organizations working with them, can use the Azure P-ATO in its own security authorization process and rely on it as the basis for issuing an agency ATO that also meets FedRAMP requirements.

Azure continues to support more services at FedRAMP High Impact levels than any other cloud provider. And while FedRAMP High in the Azure public cloud will meet the needs of many US government customers, agencies with more stringent requirements will continue to rely on Azure Government, which provides additional safeguards such as the heightened screening of personnel. Microsoft lists all Azure public services currently available in Azure Government to the FedRAMP High boundary, as well as services planned for the current year.

In addition, Microsoft is fully committed to protecting and managing customer data with clearly stated records retention policies. As a global company with customers in nearly every country in the world, Microsoft has a robust compliance portfolio to assist our customers. To view a complete list of our compliance offerings visit Microsoft compliance offering.

Authentication Basics

The following terminology is used throughout this paper.

Term	Definition
Assertion	A statement from a *verifier* to a *relying party* containing information about the *subscriber*. May contain verified attributes.
Authentication	The process of verifying the identity of a *subject*.
Authentication factor	Something you know, something you have, or something you are: Every *authenticator* has one or more *authentication factors*.
Authenticator	Something the *claimant* possesses and controls that is used to authenticate the *claimant's* identity.
Claimant	A *subject* whose identity is to be verified using one or more *authentication protocols*.
Credential	An object or data structure that authoritatively binds an identity to at least one *authenticator* possessed and controlled by a *subscriber*.
Credential Service Provider (CSP)	A trusted entity that issues or registers *subscriber authenticators* and issues electronic *credentials* to *subscribers*.
Relying Party	An entity that relies on a *verifier*'s *assertion*, or a *claimant*'s *authenticators* and *credentials*, usually to grant access to a system.
Subject	A person, organization, device, hardware, network, software, or service.
Subscriber	A party who has received a *credential* or *authenticator* from a *CSP*.
Trusted Platform Module (TPM)	A TPM is a tamper resistant module that performs cryptographic operations including key generation.
Verifier	An entity that verifies the *claimant's* identity by verifying the *claimant's* possession and control of *authenticators*.

About Trusted Platform Modules

Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. A TPM chip, or hardware TPM, is a secure crypto processor that helps you with actions such as generating, storing, and limiting the use of cryptographic keys.

Microsoft provides significant information on how TPMs work with Microsoft Windows. For more information, see this article on the Trusted Platform Module.
A software TPM is an emulator that mimics this functionality.

Authentication factors and their strengths

Authentication factors can be grouped into three categories. The following table presents example of the types of factors under each grouping.

Something you know	Something you have	Something you are
		
Password or PIN	Hardware key or phone	Facial scan or fingerprint

The strength of an authentication factor is determined by how sure we can be that it is something that *only the subscriber* knows, has, or is.

There is limited guidance in NIST about the relative strength of authentication factors. Here at Microsoft, we assess the strengths as below.

Something you know: Passwords, the most common *something you know*, represent the greatest attack surface. The following mitigations improve confidence in the affinity to the subscriber and are effective at preventing password attacks such as brute-force attacks, eavesdropping and social engineering:

- Password complexity requirements
- Banned passwords
- Leaked credentials identification
- Secure hashed storage
- Account lockout

Something you have: The strength of *something you have* is based on how likely the subscriber is to keep it in possession, and the difficulty in an attacker gaining access to it. For example, a

personal mobile device or hardware key will have a higher affinity, and therefore be more secure, than a desktop computer in an office when trying to protect against internal threat.

Something you are: The ease with which an attacker can obtain a copy of *something you are*, or spoof a biometric, matters. NIST is drafting a framework for biometrics. Today, NIST will not accept biometrics as a separate authentication method. It must be a factor within multi-factor authentication. This is since biometrics are probabilistic in nature. That is, they use algorithms that determine the likelihood that it is the same person. It is not necessarily an exact match, as a password is. See this document on the Strength of Function for Authenticators – Biometrics (SOFA-B). SOFA-B attempts to present a framework to quantity biometrics' strength in terms of false match rate, false, fail rate, presentation attack detection error rate, and effort required to launch an attack.

NIST Authenticator Types and aligned Azure AD methods

The authentication process begins when a claimant asserts its control of one of more authenticators associated with a subscriber (which may be a person or another entity).

NIST Authenticator Type	Azure AD Authentication Methods
Memorized secret *(Something you know)*	Password (Cloud accounts) Password (Federated) Password (Password Hash Sync) Password (Passthrough Authentication)
Look-up secret *(Something you have)*	None. A lookup secret is by definition data not held in a system.
Out-of-band *(Something you have)*	Phone (SMS) - *not recommended*
Single-factor one-time password (Something you have)	Microsoft Authenticator App (One-time password) Single factor one-time password (through OTP manufacturers) *
Multi-factor one-time password *(something you have + something you know or something you are)*	Multi-factor one-time password (through OTP manufacturers) *
Single-factor crypto software *(Something you have)*	Azure AD joined** w/ software TPM Compliant mobile device Hybrid Azure AD Joined** w/ software TPM Microsoft Authenticator App (Notification)
Single-factor crypto hardware *(Something you have)*	Azure AD joined** w/ hardware TPM Hybrid Azure AD Joined** w/ hardware TPM
Multi-factor crypto software *(Something you have + something you know or something you are)*	Microsoft Authenticator app for iOS (Passwordless) Windows Hello for Business w/ software TPM
Multi-factor crypto hardware *(Something you have + something you know or something you are)*	FIDO 2 security key Microsoft Authenticator app for Android (Passwordless) Windows Hello for Business w/ hardware TPM Smartcard (Federated identity provider)

* OATH-TOTP SHA-1 tokens of the 30-second or 60-second variety

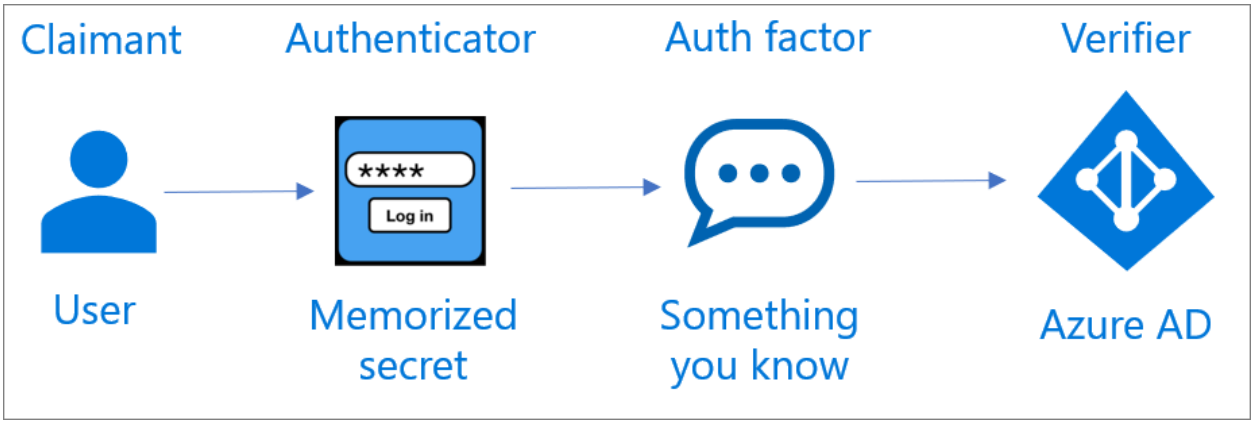
** For more information on device join states see Azure AD device identity documentation

Why SMS is not recommended

SMS text messages meet the NIST standard, but NIST does not recommend them. The risks of device swap, SIM changes, number porting, and other behaviors can cause issues. If these actions are taken maliciously, they can result in an insecure experience. While they are not recommended, they are better than using password alone, as they require additional effort for hackers.

Single-factor authentication

Single-factor authentication can be achieved by using a single-factor authenticator that constitutes something you know or something you are. While an authentication factor that is "something you are" is accepted as an authentication factor, it is not accepted as an authenticator by itself.



Multi-factor authentication

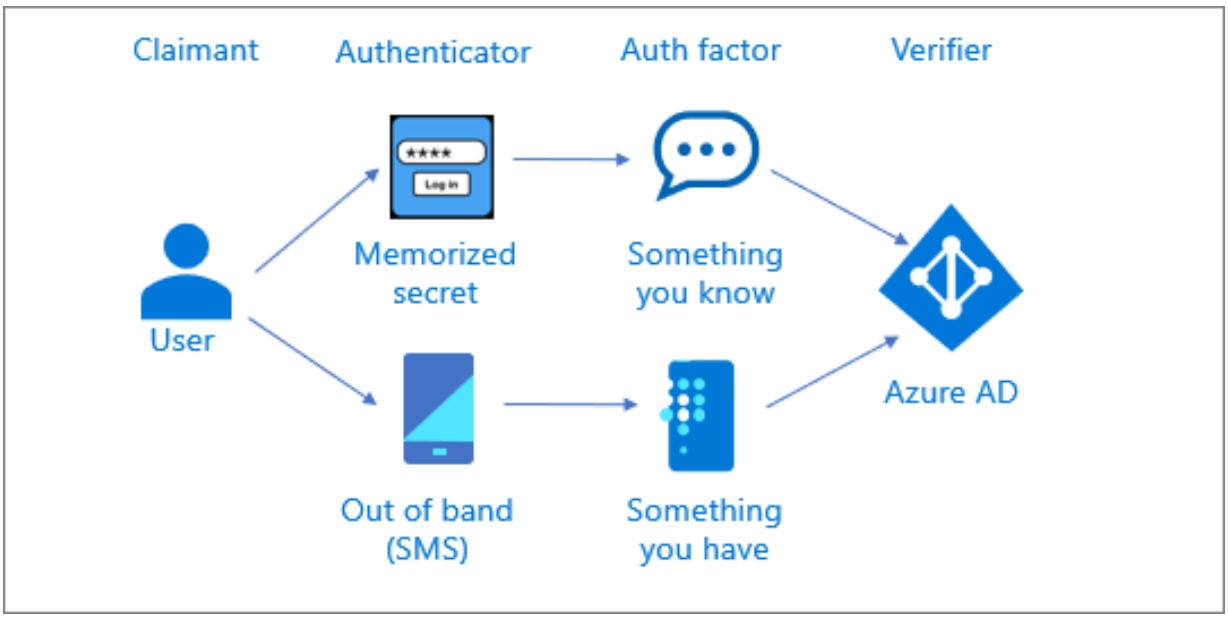
Multi-factor authentication can be achieved by either a multi-factor authenticator or by a combination of two single-factor authenticators. A multi-factor authenticator requires two authentication factors to execute a single authentication transaction.

Multi-factor authentication using two single-factor authenticators

Multi-factor authentication requires two different authentication factors. These can be two independent authenticators, such as

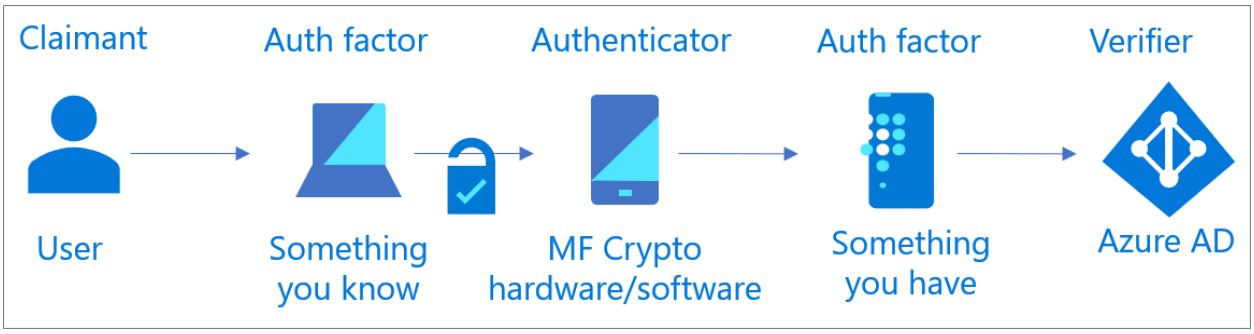
- Memorized secret [password] and out of band [SMS]
- Memorized secret [password] and one-time password [hardware or software]

These methods perform two independent authentication transactions with Azure AD.



Multi-factor authentication using a single multi-factor authenticator

Multi-factor factor authentication requires one authentication factor (something you know or something you are) to unlock a second authentication factor. This is typically a simpler user experience than multiple independent authenticators.



One example is the Microsoft Authenticator app used in the passwordless mode. With this method the user attempts to access a secured resource (relying party), and receives a notification on their authenticator app. The user responds to a notification by providing either a biometric (something you are) or a PIN (something you know), which then unlocks the cryptographic key on the phone (something you have) which is then validated by the verifier.

Achieving NIST AAL1 with the Microsoft Identity Platform

Permitted authenticator types

Any NIST permitted authenticator (single-factor or multi-factor) can be used to achieve AAL1.

Azure AD Authentication Method	NIST Authenticator Type
Password	*Memorized Secret*
Phone (SMS)	*Out-of-Band*
Microsoft Authenticator app for iOS (Passwordless) Windows Hello for Business w/ software TPM	*Multi-factor Crypto software*
FIDO 2 security key *Microsoft Authenticator app for Android (Passwordless)* *Windows Hello for Business w/ hardware TPM* Smartcard (ADFS)	*Multi-factor Crypto hardware*

FIPS 140 validation

Verifier requirements

Azure AD is using the Windows FIPS 140 *Level 1 overall* validated cryptographic module for all its authentication related cryptographic operations. It is therefore a FIPS 140 compliant verifier as required by government agencies.

Man-in-the-middle (MitM) resistance

All communications between the claimant and Azure AD are performed over an authenticated protected channel to provide resistance to MitM attacks. This satisfies the MitM resistance requirements for AAL1, AAL2 and AAL3.

Achieving NIST AAL2 with the Microsoft Identity Platform

Permitted Authenticator Types

Azure AD Authentication method	NIST Authenticator type
Recommended methods	
Microsoft Authenticator app for iOS (Passwordless) Windows Hello for Business w/ software TPM	Multi-factor crypto software
FIDO 2 security key Microsoft Authenticator app for Android (Passwordless) Windows Hello for Business w/ hardware TPM Smartcard (ADFS)	Multi-factor crypto hardware
Additional methods	
Password + Phone (SMS)	Memorized Secret + Out-of-Band
Password + Microsoft Authenticator App (OTP) Password + SF OTP	Memorized Secret + Single-factor one-time password
Password + Azure AD joined w/ software TPM Password + Compliant mobile device Password + Hybrid Azure AD Joined w/ software TPM Password + Microsoft Authenticator App (Notification)	Memorized Secret + Single-factor crypto SW
Password + Azure AD joined w/ HW TPM Password + Hybrid Azure AD Joined w/ HW TPM	Memorized Secret + Single-factor crypto HW

Our recommendations

We recommend using multi-factor cryptographic hardware or software authenticators to achieve AAL2. Passwordless authentication eliminates the greatest attack surface—the password—and offers users a streamlined method to authenticate.

For detailed guidance on selecting a passwordless authentication method, see Plan a passwordless authentication deployment in Azure Active Directory.

For more information on implementing Windows Hello for Business, see the Windows Hello for Business deployment guide.

FIPS 140 validation

Verifier requirements

Azure AD is using the Windows FIPS 140 *Level 1 overall* validated cryptographic module for all its authentication related cryptographic operations. It is therefore a FIPS 140 compliant verifier as required by government agencies.

Authenticator requirements

Government agencies' cryptographic authenticators are required to be FIPS 140 *Level 1 overall* validated. This is not a requirement for non-governmental agencies. The following Azure AD authenticators meet the requirement when running on Windows in a FIPS 140 approved mode of operation

- Password
- Azure AD joined w/ software or w/ hardware TPM
- Hybrid Azure AD Joined w/ software or w/ hardware TPM
- Windows Hello for Business w/ software or w/ hardware TPM
- Smartcard (ADFS)

FIDO2 security keys, and the Microsoft Authenticator app (in all its modes - Notification, OTP and Passwordless) do not meet government agencies requirement for FIPS 140 *Level 1 overall* validation as of this writing.

- Microsoft Authenticator app is using FIPS 140 approved cryptography; however, it is not FIPS 140 *Level 1 overall* validated.
- FIDO2 keys are a very recent innovation and as such are still in the process of the undergoing FIPS certification.

Reauthentication

At AAL2 NIST requires reauthentication every 12 hours regardless of user activity, *and* after any period of inactivity lasting 30 minutes or longer. Presentation of something you know or something you are is required, since the session secret is something you have.

To meet the requirement for reauthentication regardless of user activity, Microsoft recommends configuring user sign-in frequency to 12 hours.

NIST also allows the use of compensating controls for confirming the subscriber's presence:

- Session inactivity timeout of 30 minutes can be achieved by locking the device at the OS level by leveraging Microsoft System Center Configuration Manager (SCCM), Group policy objects (GPO), or Intune. You must also require local authentication for the subscriber to unlock it.

- Timeout regardless of activity can be achieved by running a scheduled task (leveraging SCCM, GPO or Intune) that locks the machine after 12 hours regardless of activity.

Man-in-the-middle (MitM) resistance

All communications between the claimant and Azure AD are performed over an authenticated protected channel to provide resistance to MitM attacks. This satisfies the MitM resistance requirements for AAL1, AAL2 and AAL3.

Replay resistance

All Azure AD authentication methods at AAL2 use either nonce or challenges and are resistant to replay attacks since the verifier will easily detect replayed authentication transactions since they will not contain the appropriate nonce or timeliness data.

Achieving NIST AAL3 with the Microsoft Identity Platform

Permitted authenticator types

Azure AD Authentication Methods	NIST Authenticator Type
Recommended methods	
FIDO2 security key Smartcard (AD FS) Windows Hello for Business w/ hardware TPM	Multi-factor cryptographic hardware
Additional methods	
Password **+** (Hybrid Azure AD Joined w/ hardware TPM **OR** Azure AD joined w/ hardware TPM)	Memorized secret + Single-factor crypto hardware
Password **+** Single-factor one-time-password hardware (from OTP manufacturers) + (Hybrid Azure AD Joined w/ software TPM **OR** Azure AD joined w/ software TPM **OR** Compliant managed device)	Memorized secret + Single-factor one-time password hardware + Single-factor crypto software

Our recommendations

We recommend using a multi-factor cryptographic hardware authenticator to achieve AAL3. Passwordless authentication eliminates the greatest attack surface—the password—and offers users a streamlined method to authenticate. If your organization is completely cloud-based, we recommend using FIDO2 security keys.

Please note that FIDO2 keys and Windows Hello for Business have not been validated at the required FIPS 140 Security Level and as such federal customers would need to conduct risk assessment and evaluation before accepting these authenticators as AAL3.

For detailed guidance, see Plan a passwordless authentication deployment in Azure Active Directory.

For more information on implementing Windows Hello for Business, see the Windows Hello for Business deployment guide.

FIPS 140 validation

Verifier requirements

Azure AD is using the Windows FIPS 140 *Level 1 overall* validated cryptographic module for all its authentication related cryptographic operations. It is therefore a FIPS 140 compliant verifier.

Authenticator requirements

Single-factor and multi-factor cryptographic hardware authenticators have different authenticator requirements.

Single-factor cryptographic hardware authenticators are required to be

- FIPS 140 *Level 1 overall* (or higher)
- FIPS 140 *Level 3 Physical Security* (or higher)

Azure AD joined and Hybrid Azure AD joined devices meet this requirement when

- you run Windows in a FIPS 140 approved mode of operation
- on a machine with a TPM that is FIPS 140 *Level 1 overall* (or higher) with FIPS 140 *Level 3 Physical Security*.
    - Find compliant TPMs by searching "Trusted Platform Module" and "TPM" under Cryptographic Module Validation Program.

Check with your mobile device vendor to learn about their adherence with FIPS 140.

Multi-factor cryptographic hardware authenticators are required to be

- FIPS 140 *Level 2 overall* (or higher)
- FIPS 140 *Level 3 Physical Security* (or higher)

FIDO2 security keys, Smartcards, and Windows Hello for Business can help you meet these requirements.

- FIDO2 keys are a very recent innovation and as such are still in the process of the undergoing FIPS certification.
- Smartcards are a proven technology with multiple vendor products meeting FIPS requirements.
    - Find out more on the Cryptographic Module Validation Program.

Windows hello for Business

FIPS 140 requires the entire cryptographic boundary including software, firmware, and hardware, to be in scope for evaluation. Windows operating systems are open computing platforms that can be paired with thousands of combinations of hardware. As such, Microsoft cannot maintain

FIPS certifications for each combination. The following individual certifications of the components should be evaluated as part of the risk assessment for using WHfB as an AAL3 authenticator:

- **Microsoft Windows 10, and Microsoft Windows Server** use the US Government Approved Protection Profile for General Purpose Operating Systems Version 4.2.1. from the National Information Assurance Partnership (NIAP). NIAP oversees a national program to evaluate Commercial Off-The-Shelf (COTS) Information Technology (IT) products for conformance to the international Common Criteria.
- **Microsoft Windows Cryptographic Library** has achieved FIPS Level 1 overall in the NIST Cryptographic Module Validation Program (CMVP). The CMVP, a joint effort between the NIST and the Canadian Center for Cyber Security, validates cryptographic module to FIPS standards.
- Choose a **Trusted Platform Module (TPM)** that is FIPS 140 Level 2 overall, and FIPS 140 Level 3 Physical Security. ***As an organization, it is your responsibility to ensure that the hardware TPM you are using meets the needs of the AAL level you want to achieve.*** To determine which TPMs meet the current standards, go to the NIST Computer Security Resource Center Cryptographic Module Validation Program. In the Module name field, enter "Trusted platform module." The resultant list contains hardware TPMS that meet the current standards.

Reauthentication

At AAL3 NIST requires reauthentication every 12 hours regardless of user activity, *and* after any period of inactivity lasting 15 minutes or longer. Presentation of both factors is required.

To meet the requirement for reauthentication regardless of user activity Microsoft recommends configuring user sign-in frequency to 12 hours.

NIST also allows the use of compensating controls for confirming the subscriber's presence:

- Session inactivity timeout of 15 minutes can be achieved by locking the device at the OS level by leveraging Microsoft System Center Configuration manager (SCCM), Group policy objects (GPO), or Intune. You must also require local authentication for the subscriber to unlock it.
- Timeout regardless of activity can be achieved by running a scheduled task (leveraging SCCM, GPO or Intune) that locks the machine after 12 hours regardless of activity.

Man-in-the-middle (MitM) resistance

All communications between the claimant and Azure AD are performed over an authenticated protected channel to provide resistance to MitM attacks. This satisfies the MitM resistance requirements for AAL1, AAL2 and AAL3.

Verifier impersonation resistance

All Azure AD authentication methods that meet AAL3 leverage cryptographic authenticators that bind the authenticator output to the specific session being authenticated. They do this by using a private key controlled by the claimant for which the public key is known to the verifier. This satisfies the verifier impersonation resistance requirements for AAL3.

Verifier compromise resistance

All Azure AD authentication methods that meet AAL3 either use a cryptographic authenticator that requires the verifier store a public key corresponding to a private key held by the authenticator or store the expected authenticator output using FIPS 140 validated hash algorithms. You can find more details under Azure AD Data Security Considerations.

Replay resistance

All Azure AD authentication methods at AAL3 either use nonce or challenges and are resistant to replay attacks since the verifier will easily detect replayed authentication transactions since they will not contain the appropriate nonce or timeliness data.

Authentication intent

The goal of authentication intent is to make it more difficult for directly connected physical authenticators (e.g., multi-factor cryptographic devices) to be used without the subject's knowledge, such as by malware on the endpoint.

NIST allows the use of compensating controls for mitigating malware risk. Any Intune compliant device running Windows Defender System Guard and Windows Defender ATP meets this mitigation requirement.

Next Steps

As you continue your journey in evaluating the right NIST AAL level for your organization, or segments of your organization, we encourage you to review the following documentation.

Microsoft's NIST Special Publication 800-63: Digital Identity Guidelines

NIST Identity Documents

FIPS 140-2 documentation