Hypori®

One Device, Zero Worries ™

Biometric Authentication

Introduction

Hypori offers biometric authentication because it links identity to unique physical or behavioral traits (fingerprints, face, iris) that are nearly impossible to steal, share, or forge, unlike passwords. It offers a seamless, fast user experience—replacing typing with a glance or touch—while enhancing security with high-accuracy, 99.9%+ verification rates and built-in protection against credential-based phishing.

Here is why biometric authentication is considered a preferred method:

Enhanced Security & Uniqueness

Biometric data is unique to each individual. Unlike passwords that can be stolen or guessed, biometric traits cannot be forgotten or shared.

Convenience & User Experience

It eliminates the need to remember complex passwords, reducing user frustration and increasing login speed.

Anti-Phishing & Fraud Protection

Because biometric data is not stored in the cloud in its raw form and requires the physical presence of the user (liveness detection), it is highly resistant to phishing, man-in-the-middle attacks, and credential theft.

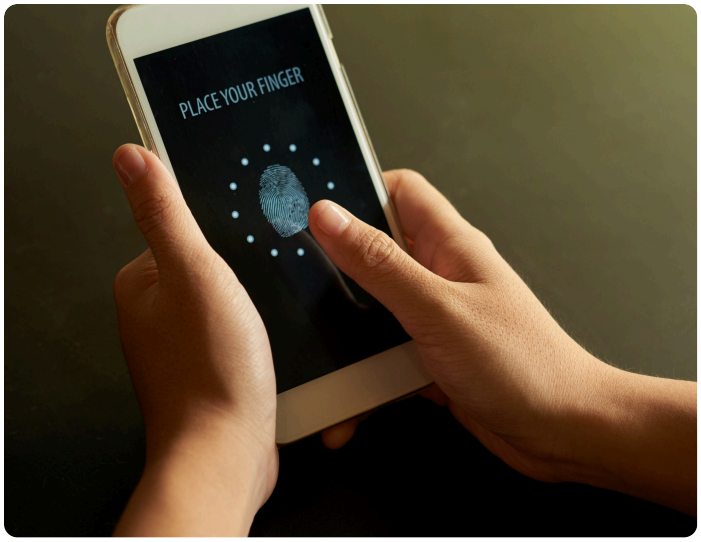
Device-Locked Security

Biometrics are typically tied to a specific device, meaning even if the device is lost or stolen, system requires both the physical device and the user to be accessed.

Cost & Operational Efficiency:

Organizations save on support costs related to password resets, while also reducing fraudulent access, improving overall security posture.

Hypori has developed Hypori Keys with Biometric Unlock, a multi-stage authentication capability protecting user access to Hypori Virtual Workspaces (VWs). Hypori Keys with Biometric Unlock is compliant with the strongest level of NIST Authentication Assurance Levels, AAL3 while greatly simplifying user experience.



How Hypori Keys with Biometric Unlock Works

Hypori Keys with Biometric Unlock leverages advanced security capabilities the Hypori Client and SaaS, end-user devices (iOS and Android) and AWS infrastructure to provide two independent stages of AAL-3 authentication to protect your Hypori Virtual Workspace while maintaining user simplicity.

Background

The National Institute of Standards and Technology (NIST) addresses this imperative through its Digital Identity Guidelines (Special Publication 800-63 series). In NIST SP 800-63B (Authentication and Authenticator Lifecycle Management), the Authenticator Assurance Levels (AALs) provide a structured framework for evaluating authentication strength:

- AAL1 offers some assurance but permits weaker methods vulnerable to phishing.
- AAL2 requires multi-factor authentication and recommends (while mandating availability of) phishing-resistant options.
- AAL3 delivers very high confidence in the claimant's control of bound authenticators. It mandates the use of a phishing-resistant authenticator with a non-exportable private key (typically hardware-protected, such as in secure enclaves, TPMs, or dedicated cryptographic devices). Authentication at AAL3 relies on public-key cryptography for proof-of-possession, replay resistance, authentication intent demonstration, and verifier impersonation resistance — explicitly designed to thwart phishing and man-in-the-middle attacks.

Adopting phishing-resistant MFA at AAL3 (or equivalent strength) significantly mitigates the dominant credential-based threat landscape.

Biometric Access

Biometric access provides a secondary authentication factor enabling the client to connect to the Hypori Virtual Workspace. The primary factor for Hypori access is always an X.509 certificate (something you have) bound to the device and store in the Trusted Execution Environment (Android) or Secure Enclave (iOS). This certificate is also the basis for the Mutual Authentication Transport Layer Security (mTLS) encrypted link protecting the connection over the internet. When configured for Biometric Access, the second authentication factor is a stored biometric (Fingerprint or FaceID) in the end user's device (something you are). To accomplish this, the Hypori SaaS sends a unique authentication challenge to the Client Application (binding it to a specific action and preventing replay attacks). The Client then calls the device's security API to authenticate the user using the device unlock method. If biometric authentication has not been locally configured, a PIN or Pattern must be used (something you know). The API confirms the identity to the Client and the Client sends an authentication token back to the SaaS allowing the connection to complete.

Semantically, it is worth pointing out that as defined in NIST 800-63, a biometric alone is not considered an authenticator but rather an activator. In the case of modern smartphones (Android with TEE or iOS) the biometric unlocks/activates the authenticator by verifying the user locally before allowing the cryptographic operation (e.g., signing with the non-exportable key). This combination satisfies multi-factor cryptographic hardware requirements: possession of the device (hardware-protected key) + biometric activation. It also provides phishing resistance and meets FIPS 140-3 equivalent hardware protections in practice for many highly regulated industry and government compliance uses.

Biometric Workspace Enforcement

When configured for Biometric Workspace enforcement, once the Client is connected to the Virtual Workspace the virtual device will immediately prompt for biometric authentication (for iOS FaceID there is no prompt and the authentication attempt happens automatically) to unlock the device. When the user sets up biometric unlock in the Virtual Workspace, the VW works through the client to register a new biometric on the user's device. Using the devices security APIs and TEE to protect the biometric data ensures that at no time is the personal biometric data transmitted to or stored in the virtual workspace.

Having a distinct biometric instance associated with the Virtual Workspace ensures that even on a device that may be shared and may for example have registered fingerprints from the authorized VW user and someone else, only the authorized VW user can authenticate into the Virtual Workspace. Without the user biometric (or PIN as a fallback) the virtual workspace remains locked and the data on it remains inaccessible. Additionally, since connection requires authenticated connection from the Hypori Client to the Virtual workspace the X.509 certificate bound to the device (something you have) has been verified.

When leveraging both Biometric Access and Biometric Workspace Enforcement, a user must satisfy two high strength authentication checks to access the Hypori Virtual Workspace. Once in the Hypori virtual workspace, Hypori can be used to support a wide variety of enterprise application authentication methods established by the customer.

So how do these features stack up against the requirements for AAL3 authentication?

Requirement	Biometric Access	Biometric Workspace Enforcement
Confidence Level	Very High	Very High
Proof of possession of a key	X.509 Cert plus Device cryptographic key (Android)/KeyChain (iOS)	X.509 Cert Device cryptographic key (Android)/ KeyChain (iOS)
Two distinct authentication factors	X.509 Cert plus Lock Screen Knowledge Factor	X.509 Cert plus Lock Screen Knowledge Factor
Hardware-based authenticator	Hardware Bound Keys in TEE/Secure Enclave	Hardware bound keys in both physical device and FIPS 140-3 validated Hardware Security Module
Phishing resistance	All keys stored in hardware and non-exportable	All keys stored in hardware and non-exportable
Approved Cryptography	FIPS 140-3 validated	FIPS 140-3 validated
Applicable permitted combination (NIST 800-63B)	Multi-factor cryptographic authenticator	Multi-factor cryptographic authenticator
FIPS 140 validation for multi-factor hardware authenticator	iOS Secure Enclave and Android TEE each FIPS validated	iOS Secure Enclave/Android TEE and AWS KMS each FIPS validated