



RANKING AUTHENTICATION METHODS

(AND CHOOSING
THE RIGHT ONE)

—

INTRODUCTION

It's no secret that cyberattacks are on the rise - and have been for some time. Even more worrisome is the unpredictable nature of these attacks, varying in form, complexity, size, intensity and even purpose. However, it's not all gloom and doom. While eliminating potential threats is not currently a feasible approach, there are resources and tools available that every organization can implement to stay best protected, reduce cyber risk, and mitigate damage.

Reported to prevent up to 90% of cyberattacks, the first step is to implement a multi-factor authentication (MFA) policy. For businesses of all sizes across all industries this is simply essential, and as of November 2021, MFA is mandatory for all federal entities per an executive order issued by the Biden administration.

TAKING THE NEXT STEP

Now that you know it's mission-critical to implement MFA, you must **take the next step** and decide which method (or methods) is right for each person both external and internal to your organization - including employees, partners, customers and third parties. While this may seem like a daunting task, we at BIO-key are here to help break down everything you need to know to take this next step with confidence.

In this guide, we explain, analyze, evaluate, and rank different methods of authentication supported by BIO-key PortalGuard® today. The following sections dive into the pros and cons of each method, with direct comparisons against one another in the following categories:

- > Security
- > Convenience
- > Cost
- > Effort of Implementation
- > Ongoing Maintenance
- > Phone-Based or Not

Interested in finding out how each method stacked up? Continue reading to explore the authentication rankings.

Using MFA can prevent up to 90% of cyberattacks, and cyber insurers and auditors are beginning to require it for private businesses.

TYPES OF AUTHENTICATION METHODS

If you're trying to make heads or tails of which authentication method is right for you and your organization, a good place to start is knowing how each method is categorized.

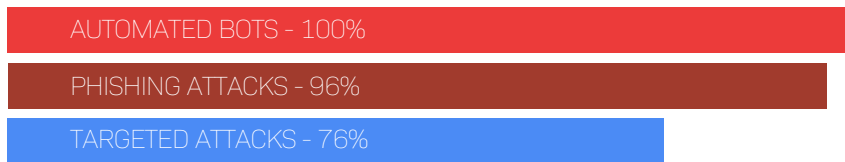
There are three main categories of authentication methods:

Something You Know: these authentication factors require a person to remember and provide something they know, such as a password or Personal Identification Number (PIN).

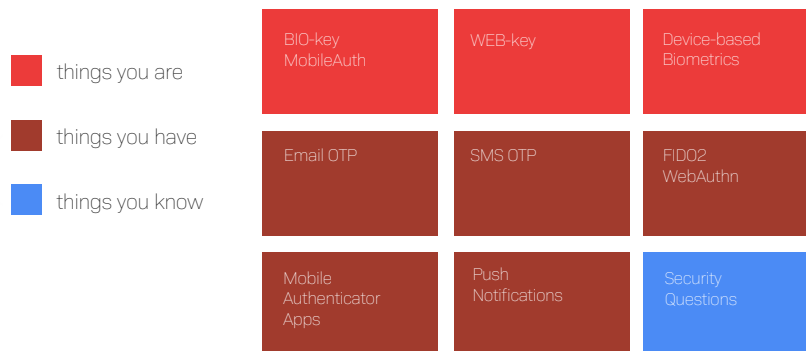
Something You Have: in this authentication scenario, the user must provide evidence of their possession of a physical item, such as a hardware token, mobile phone, or smart card.

Something You Are: this method of authentication is rooted in a piece of information inherent in the user, such as a fingerprint, palm scan or other type of biometric.

Implementing MFA can help block:



BIO-key PortalGuard supports the following authentication methods across all three categories:



Now that you know how authentication methods are categorized and defined, it's just as important to learn about the risks of picking the wrong methods and how to implement the right methods correctly.

RISKS OF PICKING THE WRONG METHOD

Having some type of MFA in place is highly recommended. — any form of multi-factor authentication (MFA) is better than no MFA at all.

That said, implementing the wrong strategy and method can impact user adoption and, in turn, overall security.

It is crucial to find the authentication method that best fits each user's needs, otherwise:



Methods that don't work for users make them hesitant or unable to adopt MFA, which is often why a one-size-fits all approach does not work.



The wrong authentication methods can create security vulnerabilities based in user gaps (pockets of users not using MFA and weak methods securing sensitive/high risk assets).



Incorrect methods lead to unnecessary rising organizational costs, as there is substantial overhead due to maintenance and multiple solutions causing operational redundancies.



Many MFA providers allow for users to accept a phone app push notification or to receive a phone call and press a key as a second factor. The Nobelium threat actor took advantage of this and issued multiple MFA requests to the end user's legitimate device until the user accepted the authentication, allowing the threat actor to eventually gain access to the account."

Mandiant Cyber Security Threat Intelligence

SIX KEY CONSIDERATIONS WHEN IMPLEMENTING MFA

At the end of the day, configuring the right security policy and choosing the right authentication strategy is a matter of fully understanding the unique needs of your organization and the best solution available.

You must be familiar with the most pressing cyber risks and confident in choosing the right authentication methods to address them. To recap, here are some key considerations to always keep in mind when implementing MFA:

- Know your users and their unique requirements.
- Assess your risk to inform your security policies.
- Have a communication strategy for implementation.
- Check your compliance and cyber insurance requirements.
- Select solutions that have multiple options vs. one-size-fits-all.
- Offer more than one option - always include one or more backup authentication methods in case the desired primary method is unavailable for any reason.

CATEGORY RANKING & ANALYSIS

Below, we've broken down and conducted a side-by-side analysis of all the BIO-key PortalGuard supported authentication methods by the following categories:

- > Security
- > Cost
- > Convenience / Ease of Use
- > Effort of Implementation
- > Ongoing Maintenance
- > Phone-based or Not

While major cybersecurity decisions take many of these into account, the vast majority of BIO-key customers rightfully consider the main two factors (Security, Usability) to be most critical in making the right decision for their authentication strategy, which are reflected in the graphic below.

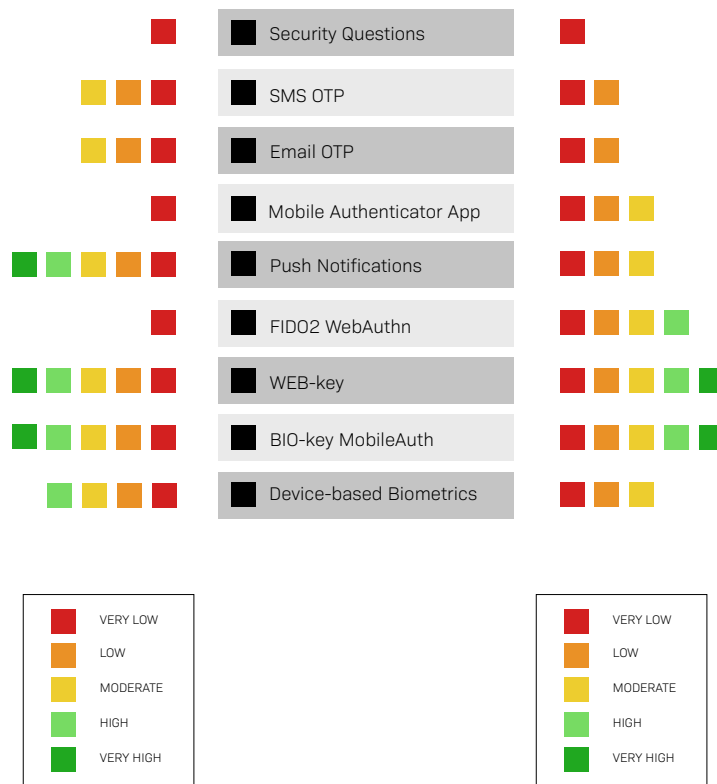
USABILITY

Ease of use increases



SECURITY

Security increases



COMPARISON CHART







While security and cost are, in fact, the top priorities for many businesses when comparing authentication solutions, there are six factors in total to consider. Below, we've analyzed and compared all of the methods by all of the six factors.

METHOD	COST	SECURITY	CONVENIENCE
Security Questions	VERY LOW	VERY LOW	VERY LOW
SMS OTP	MODERATE	LOW	MODERATE
Email OTP	VERY LOW	LOW	MODERATE
Mobile Authenticator App	VERY LOW	MODERATE	LOW
Push Notifications	MODERATE	MODERATE	HIGH
FIDO2 WebAuthn	HIGH	HIGH	LOW
WEB-key	LOW	VERY HIGH	VERY HIGH
BIO-key MobileAuth	MODERATE	VERY HIGH	HIGH
Device-based Biometrics	MODERATE	MODERATE	HIGH

METHOD	IMPLEMENTATION	ONGOING MAINT.	PHONE-BASED
Security Questions	LOW	MODERATE	<input type="checkbox"/>
SMS OTP	LOW	VERY LOW	<input checked="" type="checkbox"/>
Email OTP	LOW	VERY LOW	<input type="checkbox"/>
Mobile Authenticator App	VERY LOW	LOW	<input checked="" type="checkbox"/>
Push Notifications	MODERATE	MODERATE	<input checked="" type="checkbox"/>
FIDO2 WebAuthn	MODERATE	MODERATE	<input type="checkbox"/>
WEB-key	HIGH	LOW	<input type="checkbox"/>
BIO-key MobileAuth	MODERATE	LOW	<input checked="" type="checkbox"/>
Device-based Biometrics	LOW	LOW	<input checked="" type="checkbox"/>

WHAT'S YOUR PRIORITY?

Alternatively, if you have a certain priority in mind, such as higher security for protecting sensitive data or easy implementation because you have a smaller IT team, here are some recommendations for the authentication methods that might work best:

Solution Priority	Authentication Method
Highest Security 	<ul style="list-style-type: none"> > WEB-key IBB > MobileAuth IBB
Easiest to Implement 	<ul style="list-style-type: none"> > Mobile Authenticator App > MobileAuth IBB
Does not require a smartphone 	<ul style="list-style-type: none"> > WEB-key IBB > FIDO2 WebAuthn > Security Questions
Secure Third-Party/Supplier Access 	<ul style="list-style-type: none"> > Mobile Authenticator App > MobileAuth IBB
Secure Remote Access (VPN) 	<ul style="list-style-type: none"> > Push Notifications > Mobile Authenticator App > MobileAuth IBB > WEB-key IBB
Secure a Shared Workstation 	<ul style="list-style-type: none"> > WEB-key IBB

CONCLUSION

Implementing MFA is a key initial step in preventing cyberattacks, but deciding which methods fit your employees, partners, customers, and third parties' needs and daily workflows remains daunting. However, after understanding the ranking of each authentication method, for its security, usability, and cost, you can quickly select and deploy the best methods that fit your users.

APPENDIX: IN-DEPTH ANALYSIS OF RANKINGS

AUTHENTICATION METHOD: SECURITY QUESTIONS

Challenge Questions & Answers are one of the original and older methods of authentication. Users provide answers to previously enrolled questions.

The enrollment is completed by either an admin or the user during the first-time logging into the system.

SECURITY	CONVENIENCE	COST	IMPLEMENTATION	ONGOING MAINT.	PHONE-BASED
VERY LOW	VERY LOW	VERY LOW	VERY LOW	MODERATE	<input type="checkbox"/>

✗ Security: Very Low

Something you know is the least secure category of methods. Knowledge (answers) can be obtained via social engineering and used by anyone.

Usually, users have difficulty remembering answers and use the same question and answer combination across applications, which means when one account is compromised it can easily compromise several other accounts.

Simple answers can be easy to guess, especially with some quick research on the individual.

✗ Convenience / Ease of Use: Very Low

The user is usually required to answer 3 - 5 questions to successfully authenticate, which can take some time.

Answers can get stagnant if not used frequently and are easily forgotten after a long period of time.

Benefit: No extra devices needed.

✓ Cost: Very Low

No additional costs.

✓ Implementation: Very Low

The appropriate security questions need to be defined, as well as criteria for answers (minimum length, duplicate answers, etc.)

⊖ Ongoing - Moderate

No IT interactions should be necessary. Under normal circumstances, the user chooses and answers questions themselves.

If the user forgets the answer or submits it incorrectly, they need IT to help reset it for them. IT cannot simply reset the questions; they need to verify the user in some way first. This can be inconvenient especially for remote access.

AUTHENTICATION METHOD: SMS OTP

The SMS delivery method (often referred to simply as 'phone') involves sending an SMS text message to an enrolled mobile phone number. This SMS text message contains a One-Time Passcode (OTP) that can only be used once to validate the user for a specific action.

SECURITY	CONVENIENCE	COST	IMPLEMENTATION	ONGOING MAINT.	PHONE-BASED
LOW	MODERATE	MODERATE	LOW	VERY LOW	☒

✗ Security: Low

Susceptible to Man-in-the-Middle (MITM) attacks as SMS is sent in clear text.

Phones can be stolen. With this method, the user does not need to unlock the phone to see the text and OTP as the text contents are shown directly on the lock screen.

The SMS messages themselves can be hacked and redirected to a hacker's phone. SIM Swapping can be used to make a wireless carrier assign a different phone number to a new SIM card. SIM cards can be cloned and used in different phones.

⊖ Convenience / Ease of Use: Moderate

Almost everyone has their phone on them and easily accessible.

The code that is sent needs to be typed in. It can be easy to type it in incorrectly or not within the allotted time depending on how long/complex it is.

If your phone is out of power, you cannot authenticate. It also does not work if you do not have service. It can also take some time to receive the authentication text if service is unreliable.

⊖ Cost: Moderate

The organizations may be required to provide a phone stipend for personal devices used for authentication. The cost can be up to \$50/month per device for employees.

For availability, a hosted SMS provider should be used. For example, Twilio charges \$0.0075 per message sent/received. This is a re-occurring cost, not a one-time purchase and will increase as a business and their user base grows..

✓ Implementation: Low

Little is needed on the IT side other than setting up the hosted SMS service provider.

✓ Ongoing: Very Low

IT will only need to update phone numbers if a user gets a new one, which is uncommon.

The hosted SMS provider is responsible for disruptions in service, but any disruptions will affect users and there will be IT resources required to manage access and communications during any disruptions/outages.

AUTHENTICATION METHOD: EMAIL OTP

The Email OTP delivery method involves sending an email to an enrolled email address. This email contains an OTP to validate the user for a specific action.

SECURITY	CONVENIENCE	COST	IMPLEMENTATION	ONGOING MAINT.	PHONE-BASED
LOW	MODERATE	VERY LOW	LOW	VERY LOW	<input type="checkbox"/>

Security: Low

Best practices require that the application you are trying to access is not the source of the second factor of authentication. This is for security and usability issues. For example, if you are trying to login to PortalGuard and get Single Sign-On (SSO) into your applications, including email, then receiving the code to your email is not feasible.

The email can easily be intercepted with a Man-in-the-Middle (MITM) attack.

The application being signed into is inherently trusting that the user's email is not compromised, which sometimes may be the case especially with the rise of phishing attacks.

Convenience / Ease of Use: Moderate

Users trying to login to access email will be unable to receive the OTP via email as explained above.

Delivery is based on SMTP relay which could cause a delay based on the connection.

Spam filters/email filters will often catch these emails requiring the user to search for the email or be unable to receive it.

Cost: Very Low

There are an abundance of free SMTP relays (e.g., Gmail, Office365, Yahoo)

Many organizations already have an internal SMTP relay, as this is the most secure option.

Implementation: Low

To integrate with an SMTP relay is quick and easy if you're using a public relay (not recommended for production). More needs to be managed if you're using your own internal relay, but this is not time consuming either.

Ongoing: Very Low

There is more responsibility for IT compared to the SMS OTP method as you would not have a service provider managing the SMTP for you.

AUTHENTICATION METHOD: MOBILE AUTHENTICATOR APPS

These applications generate a Time-Based One-Time Passcode (TOTP) and are installed on the user's device. When authenticating the user will be prompted to locate and open the app on their device and then enter in the TOTP that is shown.

SECURITY	CONVENIENCE	COST	IMPLEMENTATION	ONGOING MAINT.	PHONE-BASED
MODERATE	LOW	VERY LOW	VERY LOW	LOW	<input checked="" type="checkbox"/>

Security: Moderate

The only viable attack is a brute force attack (PortalGuard has built-in defenses against this in the form of strikeout limits and account lockouts).

If the secret key is obtained by a hacker, no attack is needed as they will have access to all OTPs that are generated until the key is replaced.

Convenience / Ease of Use: Low

It is simple to enroll, with most applications utilizing a QR code to initiate the enrollment.

Each code usually lasts 30 seconds which can be too little for users who are trying to type in the code before it expires.

Most - but not all - implementations accept 1 or 2 code cycles earlier to account for any clock sync issues.

Even though most authenticator apps are used on mobile devices, if you use a desktop TOTP authenticator app, you can copy and paste the code quickly versus typing it in.

Cost: Very Low

The organization may be required to provide a phone stipend for personal devices used for authentication. The cost can be up to \$50/month per device for employees.

There are a lot of free options such as Google Authenticator and Microsoft Authenticator.

There are various paid "premium" apps, such as Twilio, Authy, and DUO Security.

Implementation: Very Low

PortalGuard only requires the simple and easy checking of a box to enable this method.

Ongoing: Low

The only IT requirement would be if a user gets a new phone, or is unable to access the mobile app. The old secret will need to be forgotten and a new one created.

AUTHENTICATION METHOD: PUSH NOTIFICATIONS

A push token is an 'out-of-band' second factor tied to a mobile device. This second factor allows end-users to confirm or deny an authentication request by interacting with their mobile device in real-time. No codes need to be remembered - just tap yes or no on the screen to confirm the authentication request.

SECURITY	CONVENIENCE	COST	IMPLEMENTATION	ONGOING MAINT.	PHONE-BASED
MODERATE	HIGH	MODERATE	MODERATE	MODERATE	<input checked="" type="checkbox"/>

⊖ Security: Moderate

- Very secure, MITM attacks are not possible.
- Out-of-Band is more secure requiring the use of a separate device.
- Push notifications are not tied to the individual which can be problematic if a phone is stolen or lost.
- A lot of phones have biometric authentication built in. Ex. TouchID, FaceID
- User could see if someone tried to access their account if they receive a push when not trying to sign in.

✓ Convenience / Ease of Use: High

- Most people have their phones on them or close by.
- This method does not require the phone to have service or internet connection.
- There is no need to type in a code. It is a simple Accept or Deny with a tap of the screen.
- Push notification appears right on your phone without opening it.
- No way to intercept.

⊖ Cost: Moderate

- The organization may be required for provide a phone stipend for personal devices used for authentication. The cost can be up to \$50/month per device for employees.
- Paid services can be costly, such as Twilio Authy (\$0.09/auth) and DUO Security (\$3-\$9/user/month).
- The cost can quickly add up with larger environments and can be difficult to predict when your organizations scales quickly.

⊖ Implementation: Moderate

- This method does need to be integrated using an API with PortalGuard. PortalGuard already integrates with BIO-key MobileAuth, Twilio Authy, and DUO Security "out-of-the-box".

⊖ Ongoing: Moderate

- Depending on the provider, some IT effort will be needed to enroll users.

AUTHENTICATION METHOD: FIDO2 WebAuthn Hardware Tokens

FIDO2 (AKA WebAuthn) differs from FIDO U2F in that it is designed for a passwordless approach to secure authentication. Functionally, FIDO2 tokens support the same usage as FIDO U2F, though utilizing a different industry standard and browser-based API. FIDO2 Tokens support one of two usage types: Click to Authenticate or On-Device Authentication. Click to Authenticate requires a tap/click of the token while On-Device Authentication detects the FIDO2 request and automatically responds, allowing the authentication action to proceed without any additional actions from the user.

SECURITY	CONVENIENCE	COST	IMPLEMENTATION	ONGOING MAINT.	PHONE-BASED
HIGH	LOW	HIGH	MODERATE	MODERATE	<input type="checkbox"/>

✓ Security: High

Something you have does not verify the individual using the token. Some tokens do have biometric scanners integrated into the token in the form of a fingerprint sensor, however, those simply verify the biometric on the device, and do not verify the biometric centrally with your organization.

The level of security relies on the proper handling of the token by the user. Tokens can be easily stolen, shared, or lost.

If the workstation being accessed is shared, the tokens are often left in the USB slot on the station allowing sharing and access to many users for the same token.

✗ Convenience / Ease of Use: Low

These stand-alone hardware tokens are easily lost. They are commonly left in the USB ports in shared computers. This causes both a security risk but also an inconvenience to users and IT.

The process of authenticating is relatively easy with a simple plug in the device and one tap authentication workflow.

Tokens can be used for passwordless authentication for convenience. However, this would be considered a single factor authentication if it is not combined with anything else.

✗ Cost: High

There is a one-time cost of purchasing the tokens, with prices ranging from \$25 to over \$100 for FIPS Verified for a single token.

FIPS Verified are often needed for some government organizations or contractors. Other organizations may require it if desired.

When purchasing tokens, it is recommended to purchase 2-3 per user. This accounts for lost/broken keys.

As your organization scales, more tokens will need to be purchased.

Often a bulk discount is available for larger quantities depending on the vendor.

⊖ Implementation: Moderate

IT needs to purchase, distribute, and manage the hardware keys.

Most applications can do self-service enrollment, but some would require IT to pre-enroll the tokens for their respective user accounts, which can be time consuming.

⊖ Ongoing: Moderate

If a key is lost, IT needs to clear the current token out of the system so it cannot be used as well as issue a new one.

AUTHENTICATION METHOD: WEB-key (Identity-Bound Biometrics)

WEB-key is an enterprise-grade Identity-Bound Biometrics platform from BIO-key. IBB creates a centralized unique biometric identity that can be used to verify you anywhere. The primary method for capturing the biometric is by using a fingerprint scanner.

SECURITY	CONVENIENCE	COST	IMPLEMENTATION	ONGOING MAINT.	PHONE-BASED
VERY HIGH	VERY HIGH	LOW	HIGH	LOW	<input type="checkbox"/>

✓ Security: Very High

Enterprise-controlled enrollment prevents account handovers and ensures only approved individuals can use account privileges.

There is a decreased susceptibility to common authentication attacks, as IBB authentication methods cannot be forgotten, shared, exchanged, stolen or forged.

Biometric data privacy is ensured through irreversible, cryptographic hashing and salting to render the information inaccessible and usable for potential bad actors.

Built-in liveness detection provides strong Presentation Attack Detection (PAD) by imposters trying to use scanned pictures or fakes.

IBB eliminates concerns around a single point of failure by removing physical devices as potential vulnerabilities (as present with local or device-native biometrics).

✓ Convenience / Ease of Use: Very High

Supports a broad range of use cases and provides a more consistent experience for all users.

Only a one-time enrollment is required to setup access across multiple devices and locations.

Supports roving users accessing secured systems on shared workstations.

Offers easy to use options when phone-based methods do not work or are not permitted.

Supports multi-factor authentication when your server is offline, using PortalGuard Desktop.

✓ Cost: Low

One-time purchase of fingerprint scanners with no recurring costs like hardware tokens, resulting in low total cost of ownership (TCO) for large scale deployments.

Affordable and quick to implement at any scale with straightforward pricing to achieve measurable ROI in 90 days or less.

✗ Implementation: High

It takes some additional effort to setup. The WEB-key server needs to be stood up and configured, alongside the WEB-key software being installed on workstations.

Fingerprint scanners need to be purchased and distributed, with the drivers also being installed.

✓ Ongoing: Low

There is minimal WEB-key server maintenance since it must be self-hosted.

Most of the IT effort involved is in the initial setup. Once it's going there is little IT interaction needed. All actions are self-service except backend administrator actions.

AUTHENTICATION METHOD: BIO-key MobileAuth (Identity-Bound Biometrics)

BIO-key MobileAuth is an easy-to-use MFA mobile app with no new hardware required and a fast QR code registration and enrollment process that can be completed in seconds. MobileAuth offers PalmPositive as an authentication method and form of Identity-Bound Biometrics which uses a simple palm scan to authenticate the individual.

SECURITY	CONVENIENCE	COST	IMPLEMENTATION	ONGOING MAINT.	PHONE-BASED
VERY HIGH	HIGH	MODERATE	MODERATE	LOW	☒

✓ Security: Very High

A palm scan is 400x more accurate than Apple Touch ID and related technologies.

Combines 'something you have' AND 'something you are' for heightened security.

Identity-Bound Biometrics is tied to the individual – not a device – which means credentials cannot be stolen, intercepted, forged, forgotten, or exchanged.

✓ Convenience / Ease of Use: High

A fast and easy QR code registration and enrollment process that takes only a few seconds.

You do need to pull your phone out to access the push notification and scan your biometric each time you authenticate.

⊖ Cost: Moderate

Phone stipends for employee phone plans can cost up to \$50/month per device.

⊖ Implementation: Moderate

Users will need to download the BIO-key MobileAuth app and enroll it within PortalGuard as directed by IT.

Basic configuration will need to be done with the BIO-key PortalGuard team to enable this in the PortalGuard security policies.

✓ Ongoing: Low

Ongoing maintenance is minimal for IT. Users will need to download the app if they get a new phone or loses/breaks their current one.

AUTHENTICATION METHOD: Integrated Device-Based Biometrics

Integrated device-based biometrics refers to biometric methods where all processing, matching, and authenticating of the biometric is completed on the device. This includes methods such as Touch ID and Face ID on iOS devices, biometric authentication on Android devices, and Windows Hello on Windows devices.

SECURITY	CONVENIENCE	COST	IMPLEMENTATION	ONGOING MAINT.	PHONE-BASED
MODERATE	HIGH	MODERATE	LOW	LOW	☒

⊖ Security: Moderate

These system-on-a-chip integrated biometrics are not the most secure as what is authenticated to the relying party is often the device certificate or token, instead of the actual biometric (aka the person) being verified.

This can almost always be bypassed with a password or PIN. This means it is only as secure as the PIN.

The user is the one who is in control of the enrollment of any biometrics on the device, allowing for unauthorized users to be enrolled without the relying party knowing, removing any level of trust that only authorized users are gaining access.

✓ Convenience / Ease of Use: High

Integrated into the user's device. This method is used to unlock the device and perform various other tasks every day.

Many people are comfortable, familiar, and are already enrolled to use this type of authentication, making it feel like second nature to users.

No installation and little configuration are needed.

Users have to enroll and configure every individual device as the authentication is tied to the specific device the biometric is captured on. For this reason these biometric methods are inconvenient when users have multiple devices, use shared workstations, and/or work across multiple locations.

⊖ Cost: Moderate

Smartphones with integrated biometrics can be very expensive, especially compared to phones without that feature. For employers, phone stipends may be required and can cost up to \$50/month per device.

Windows Hello biometrics require a built-in fingerprint scanner or specialized camera. Devices, such as laptops with these built-in features can cost more than those without. For example, a standard built-in webcam cannot be used for facial recognition, as it cannot detect depth and liveness, requiring that a separate device be purchased.

✓ Implementation: Low

Since these methods are native to the device, little or no implementation is required. There is no additional installation, and the user simply needs to enroll his or her face/fingerprint with the built-in scanner or camera.

✓ Ongoing: Low

IT needs to supply the devices to enable biometrics. There may be support required to help users enroll on every device or location they are trying to access since authentication is handled locally.

ABOUT BIO-KEY INTERNATIONAL

BIO-key International is a trusted provider of Identity and Access Management (IAM) and Identity-Bound Biometric solutions that enable convenient and secure access to devices, information, applications, and high-value transactions. BIO-key offers the simplicity and flexibility required to secure the modern digital experience for on-prem and remote users, while easing the burden on IT teams.

BIO-key PortalGuard is a fully unified Identity-as-a-Service (IDaaS) platform with industry-leading biometric identity options, single sign-on, multi-factor authentication, adaptive authentication, and self-service password reset. Backed by decades of expertise, BIO-key has a proven track record of successful IAM project delivery, strong partner relationships, and low TCO.