opentext™

GUIDE

Passwordless Buyer's Guide

A practical guide to reducing risk and friction in digital identity

Contents

Authentication stands at the intersection of user experience and security. Yet, for many organizations, traditional credentials—usernames and passwords—remain the weakest link in their identity ecosystems. Despite being easy to deploy, passwords are vulnerable to phishing, theft, reuse, and fatigue. As cyberthreats become more sophisticated and user expectations for seamless experiences grow, the shift toward passwordless authentication has become a strategic necessity.

This buyer's guide is designed to help organizations confidently evaluate and implement passwordless solutions that align with their business, risk, and user experience needs. Whether you're looking to secure enterprise workflows, streamline B2C interactions, or reduce operational costs, this guide offers a practical, comprehensive framework for choosing authentication methods that balance usability with assurance strength.

We explore the broad landscape of passwordless technologies—from biometrics and mobile push authentication to cryptographic keys and behavioral analytics—and evaluate each against criteria such as security strength, friction level, and administrative overhead. We also provide insight into assurance levels as defined by NIST and how they influence authentication strategy, especially in regulated industries.This guide aims to empower IT leaders, CISOs, and identity architects to modernize access control without compromising on protection.

The business impacts of passwordless

The fact that traditional credentials are essentially free and easy to create ensures their continued use, yet their shortcomings have forced many organizations to do more to make authentication stronger and simpler.

Users get irritated when confronted with a cumbersome authentication request that slows them down. When they perceive authentication as unwieldy, they'll often try to scheme workarounds, which may compromise security.

Higher level of security

Because they can be phished or stolen, traditional credentials create a breach risk or other types of digital service disruption. Also, because users may reuse credentials from their personal accounts to their professional ones, passwords compromised on a user's less secure personal service may create a vulnerability. It's even a greater risk in B2C services, where credential sharing is quite common.

While passwordless technologies have long been used for multi-factor authentication, used on its own, even single-factor passwordless authentication offers some advantages over traditional usernames and passwords.

Passwordless methods rely on factors like biometrics (fingerprint, facial recognition) or possession (security key, smartphone) that are unique to the user or difficult to replicate. Possession factors, such as security keys, require physical possession, adding an extra layer of security.

	Traditional username and password	Passwordless
Vulnerable to phishing	Yes	No
Inherent security strength	Weaker – can be phished, stolen, may be shared across internet services	Stronger – unique or possession-based
Single point of failure	Password can be reset	Likely more difficult to recover
Universally applicable	Yes	May not work for everyone
Maturity of technology	Well established	Evolving

Comparing traditional credentials to passwordless technologies

While passwordless authentication relieves users from the complexity of remembering one of many credentials, it does have its limitations. The devices themselves need to be tightly secured, and resetting these environments is far more complex than resetting someone's password. Additionally, biometric authentication types may not work for everyone due to physical limitations, types of daily activities, or disabilities.

Increasing business efficiency

Implementing the right type of authentication has the potential to do more than improve security. It can boost productivity, lower costs, and streamline operations. With the right fit, passwordless authentication can remove friction from traditional logins, giving employees fast, seamless access to sensitive information. Eliminating traditional credentials, password entry and reset delays, helps organizations speed up daily tasks, leading to smoother workflows and allowing employees to focus on core responsibilities instead of login issues.

Replacing manual credential entry with a single gesture or biometric scan also removes frustration, especially on mobile devices. When users can start work instantly and without hassle, it improves morale and reduces login fatigue, leading to higher engagement.

Faster onboarding, quicker service, and reduced internal delays help companies outperform slower competitors. Passwordless authentication supports agility, responsiveness, and innovation—all key traits in a digital-first marketplace.

Passwordless authentication for B2C digital interactions

Passwordless authentication can significantly improve business-to-consumer (B2C) interactions, allowing for more effective engagement. Consider two competitive mobile apps requiring secure access controls to protect sensitive information.

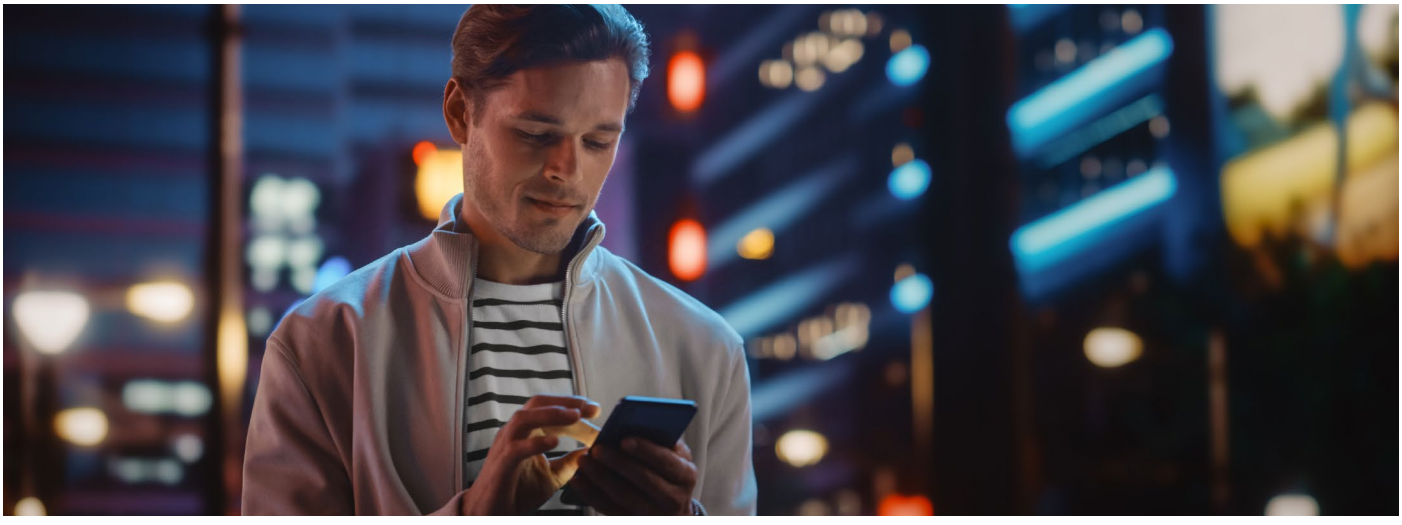
The simple app is accessed with a touch of a finger or a scan of an iris. The cumbersome app requires the consumer to enter a long password enforced with a policy that forces a mix of uppercase and lowercase letters, numbers, and symbols, and requires them to be changed every number of days. One app puts up access roadblocks while the other is undemanding without compromising the strength of security.

How authentication adaptability affects your passwordless strategy

Generally, the more securely you lock a digital resource, the bigger the hassle users have accessing it. As you develop your authentication strategy, think about use cases such as:

- Should a user have to authenticate to take a quick scan at the cafeteria menu or corporate information that is publicly available?
- Does it make sense to disrupt a person accessing low-risk information with a complex identity verification step?
- Are there better ways you can interact with your digital consumers?
  - Use a simple app, device, or other tags to deliver personalized information without disrupting the user.
  - Unless information is covered by a government mandate, use a passive authentication type when risk levels allow.
  - Make greater use of context and historical context to raise confidence in the claimed identity and control the authentication experience based on it:
    - Geolocation
    - IP address range
    - Other HTTP header information
    - Geofencing
    - Device ID
    - Browser cookies

Just as important as a solid set of risk-based metrics to determine the appropriate verification strength is providing various authentication options. Users allowed to enroll for multiple authentication types are given greater flexibility while the organization benefits from the strongest authentication experience. Implementing a risk-based environment without multiple authentication options is a mismatch of investment.



Vetting your assurance levels

Before designing a passwordless strategy, you need to understand the level of assurance required to protect your sensitive data. The pitfalls of treating all pieces of information alike is that you incur extra cost and efficiency penalties by locking down information that should be more freely accessible or you create vulnerabilities by under securing access to your most sensitive data.

The strength of protection needed involves thinking about how much harm would result if someone gained unauthorized access to your data. For example, a breach of general process internal documents versus R&D or consumer financial information.

You also have to consider regulations and compliance required for certain types of data. For instance, healthcare data falls under HIPAA (Health Insurance Portability and Accountability Act) in the US, and financial data may be subject to PCI DSS (Payment Card Industry Data Security Standard). These regulations often mandate the minimum level of security required.

Here's a recommended approach to assess your data security needs:

Identify your sensitive data: Make a list of all the data you hold that could be damaging if compromised. This could include financial information, personal details (like Social Security numbers), intellectual property, or confidential business documents.

Classify the data: Once you've identified your sensitive data, categorize it based on the potential impact of a breach. For example, data with severe consequences (like financial records) would be considered high risk, while lower-risk data might be meeting minutes or internal reports.

Don't forget regulations and mandates: Research any industry regulations or compliance requirements that apply to your data. These will dictate the minimum security measures that you must implement to stay compliant, for protecting against violation findings and even fines.

While vetting your data for assurance levels is needed for your passwordless deployments, it's not a one-time exercise. Conducting data classification regularly is a must to properly secure potentially sensitive information.

Setting the authenticator stage with assurance levels

Before you can review and assign data to the proper access security level, you need to understand the guidelines. This buyer's guide starts with NIST's (National Institute of Standards and Technology) authentication criteria as described in SP 800-63B to assign levels of security. NIST's Authentication Assurance Level (AAL) assigns an authentication strength based on the sensitivity of the protected information. The higher the AAL level, the greater the confidence that the claimed identity has been successfully verified.

Authenticator Assurance Level 1—some assurance (AAL1)

AAL1 is defined as "provides some assurance that the claimant controls an authenticator bound to the subscriber's account." The common uses of this level of identity assurance are to control access for general business information that is classified as minimal impact in case of a compromise, or consumer personalized information that doesn't contain the customer's private information. For this level of assurance, the following passwordless authentication types are most commonly in single-factor use cases that satisfy this level of identity assurance:

Look-up secret – like numeric or character strings printed on a card in table format. It represents something you have.

Out-of-band device – a physical device (typically a smart phone) that is uniquely addressable and can communicate securely with the verifier over secondary channel. It represents something you have.

One-time password (OTP) device – using a secret as a seed, the software on the device, such as a smartphone, generates the PINs that can only be used once. The displayed OTP needs to be manually entered, proving possession and control of the enrolled device.

Authenticator Assurance Level 2—high confidence (AAL2)

AAL2 is designed to provide a higher degree of confidence that the person attempting to access a system or resource is who they claim to be. As such, most of the use cases require that two authentication factors be used that adhere to secure authentication protocols. To reach this level of assurance, a combination of at least two of the following three factors are required:

- **Something you know:** A PIN, password, or security question.
- **Something you have:** A hardware token, a software token, or a one-time password (OTP) generator.
- **Something you are:** Biometric identifiers like fingerprints, facial recognition, or iris scans.

AAL2 also requires that replay resistance be implemented; meaning that at least one of the authentication factors cannot be used multiple times to gain unauthorized access.

In their classification, NIST allows two of these techniques to be used in AAL2 situations with just a single factor. Software cryptographic authenticators, such as mobile app-generated, time-based, one-time passwords (TOTPs) or hash-based one-time passwords (HOTPs), are classified as high confidence assurance. The most popular of which are Google Authenticator, Microsoft Authenticator, and Authy. They use cryptographic algorithms to generate codes that are unique and time sensitive, making them difficult for attackers to guess or intercept. To maintain that level of trust, it's essential that these cryptographic software authenticators do not allow the cloning of the secret key onto multiple devices.

A single-factor cryptographic device can also provide AAL2 security. These hardware devices perform cryptographic operations using protected cryptographic key(s) and provide the authenticator output via direct connection to the user endpoint. To protect against unintended confirmation, these cryptographic device authenticators should require a physical input (e.g., the pressing of a button) to operate. As these devices continue to evolve, it's becoming more common for the buttons on these devices to double as fingerprint readers, a clever way to add another factor without any additional friction.

The FIDO Alliance (Fast Identity Online Alliance) is an industry consortium founded in 2012 to develop and promote open authentication standards that reduce reliance on passwords. Its purpose is to enhance security and user convenience through strong authentication methods, such as biometrics and hardware security keys, using public-key cryptography. In 2014, it introduced the FIDO Universal Authentication Framework (UAF) and Universal Second Factor (U2F) protocols, enabling passwordless and two-factor authentication.

By 2018, the alliance upgraded U2F to Client to Authenticator Protocol (CTAP) and worked with the World Wide Web Consortium (W3C) to create FIDO2. FIDO2 enables passwordless authentication across web and mobile platforms.

FIDO2 enables passwordless authentication, eliminating weak and easily compromised credentials. This removes the need to remember and manage multiple passwords and builds on the alliance's objective of making authentication phishing-resistant while increasing its usability.

One of FIDO2's more attractive features is its cross-platform compatibility, working seamlessly across various operating systems, web browsers, and hardware devices. Major tech giants, such as Google, Microsoft, and Apple have since adopted FIDO2 and integrated it into their ecosystems, allowing users to authenticate securely using built-in device authenticators or external security keys.

The standard also aligns with regulatory requirements for strong authentication, making it an ideal solution for businesses seeking to enhance security and comply with industry's best practices.

Authenticator Assurance Level—very high confidence (AAL3)

AAL3 requires users to provide something you know + something you are. Because it requires two independent factors, one of which is a biometric factor, it is the strongest level of identity assurance. Until recently, AAL3 authentication was rarely used, but modern smartphones have changed that. Today, passkeys and other types of authenticator apps commonly require AAL3 identity verification when a user accesses sensitive information from an unknown device or unexpected location. Here is the common use case:

- The user authenticates to a service that delivers out-of-band confirmation of the user's identity beyond the user's claim and password.
- The authenticator service determines if the device is known or has a valid token.
- Depending on the policy setup, if the device is known or token is valid, all the user must do is approve the request from the authenticator app.
- If the token is expired, the user must comply with a biometric (fingerprint, facial recognition, or iris recognition) before providing the number or code (something that is known) and approval.
- The added step of providing a number protects against attackers attempting to use authentication request fatigue as a strategy for getting a user to simply approve.

AAL3 is also possible as a purely passwordless experience. The user:

- Has possession of an enrolled device (something the user has).
- Provides a biometric confirmation (something the user is).
- Matches the number option provided by the requested service (something the user knows).
- Confirms intent with approval.

Selecting the authentication experience that best fits your business

While no two organizations have the same mix of priorities, this guide assesses the most common criteria authentication teams use as they review

Assurance strength

Since the No. 1 credential attack vector is phishing, it's a key factor in rating assurance strength. Encryption and secure communication protocols needed to protect the authentication data during transmission and storage are other criteria.

While essential, device security falls outside of assurance strength. Device security is accomplished through configuring features on the device itself.

Usability

User convenience is a core component for broad adoption. A passwordless experience needs to be simple to set up and maintain and offer a straightforward way to recover when it fails. It must have low or no friction, such as cumbersome steps or repeated prompts.

These interruptions frustrate users, reduce productivity, and often lead to increased helpdesk costs. For customers, friction can drive abandonment.

Administrative complexity

This category covers everything from deployment and user enrollment to ongoing administration and potential limitations (such as complexion limitations) that may apply to a segment of the user base.

At the end of each method type reviewed throughout the rest of this paper are ratings given per the criteria described above. While the ratings can't be applied to every situation, they do serve as a starting point for evaluating them for your environment.

Excellent | **Very good** | **Average** | **Below average** | **It's a concern**

Hard tokens

Authentication using a hard token involves a hardware device capable of displaying a time-based pin. After a hard token has been assigned to a user, they use the time-based pin being displayed to complete the requested factor in the authentication process. As a variation, OATH-based hardware tokens use open standards like HOTP (HMAC-based One-time Password) or TOTP (Time-based One-time Password) to generate the PIN or code. OATH-based hardware tokens are generally viewed as more affordable than traditional tokens, but their open-standards approach makes them less tamper-proof compared to FIDO2 token's nature. The OATH standard also makes these tokens more versatile and compatible with a wider range of services and systems.

Once the dominant method for two-factor authentication, today, the use of hardware tokens is far more specialized. While hard tokens offer strong security, usability and overhead costs have limited their use:

- Same level of friction as other visual tokens
- Enrollment requires an administrator to manually assign a device to a user and then send it to him.
- When a token requires support or troubleshooting, it may involve the user sending the device back to central IT, which is inconvenient and more expensive.
- Users may prefer accessing a token from their phone, which they're already carrying with them, rather than carrying yet another device.

The potential for a token needing to be shipped back and forth between the user and administrator raises the need to have a backup 2FA option. And since hard tokens tend to be used in higher security situations, the alternatives need to be strong enough to meet your security needs.

Since the use of multi-factor authentication is far more pervasive now than when hard tokens were first adopted, other authentication types may need to be deployed across the organization to control costs and administrative overhead. Not all tokens have the same level of protection against theft and some styles openly display the current token, others first require some type of challenge-response.

- The physical nature of a token increases administrative overhead.
- Gaps in remote administration mandate the need to have a backup authentication type available.

Mobile SMS (one-time PIN)

Today, short message service (SMS) one-time PIN (OTP) is the most common type of two-factor authentication. Its popularity is largely driven by the availability of databases with phone numbers, the relatively low cost of deployment, and entry-point devices. Most individuals performing transactions own a mobile device and are familiar with SMS. It capitalizes on the fact that people usually keep their phones with them.

There are three different foundation points to SMS-based OTP's security model:

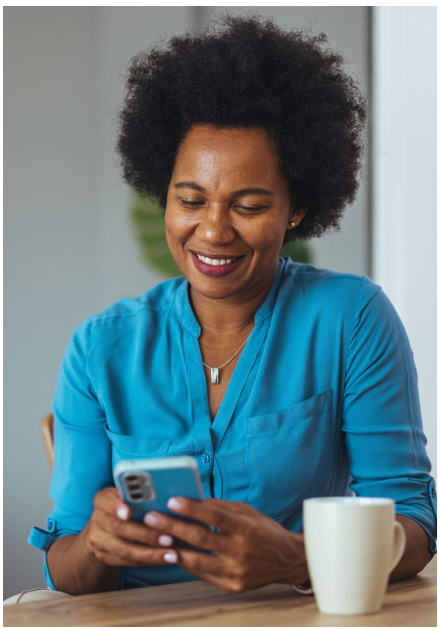
- The owner's identity was verified when it was assigned to a specific SIM (subscriber identity module) card or built-in SIM, which are tied to a phone number.
- The OTP is a separate verification point that is received out-of-band from the initial entry of the user's credential. So, even if the credential has been hacked or phished, the security of the SMS PIN is unaffected.
- OTPs are commonly four to six digits long and virtually always time-based. The lifespan of an OTP is typically short, making them outdated and worthless for identity verification after they have expired.

SMS's big usability advantage is that people get texted all the time, so getting an OTP isn't that different. The user doesn't have to install an app and onboard a device; rather, simply add their mobile number to their account. Friction of SMS is the same as other PIN authentication options.

While mobile SMS-based OTPs are one of the most common multi-factor authentication options, they do have vulnerabilities. Although more difficult than hacking passwords, they are vulnerable to man-in-the-middle scenarios. SIM swapping is another risk that has seen notable growth in recent years. Social engineering poses a risk with most authentication methods, but especially SMS, which doesn't require verification of the person's messages. It's also dependent on strong security on the device itself in case of device theft.

- Easy to administer
- Inexpensive to deploy
- Straightforward for the user learn

Assurance strength	Usability	Administrative overhead



Mobile app (out-of-band push and TOTP)

Out-of-band push and TOTP (time-based one-time password) are grouped together in this guide because they are commonly provided together. It's common for mobile apps to offer TOTP as both an option and a backup when a cell connection isn't possible. While OTP can be generated based on various factors like counters or events, TOTP relies on the current time to generate the code.

Authentication through an out-of-band mobile app differs from SMS in that before it can be used, the users must first securely enroll their instance (device) with the identity provider (IdP) within the service. The key difference is that because the TOTP is sent to the user's mobile app rather than a phone number, both the service provider and the user are protected against SIM swaps or other man-in-the-middle attacks. These out-of-band mobile apps typically offer one-time PINs as well as an approval option when an out-of-band push notification is received. Since these notifications are sent using an encrypted protocol, they provide a higher level of security. Additionally, in most situations, approving a push notification is faster and more convenient than typing in a PIN.

These mobile apps typically require the recipient to verify their identity to access them, usually with a fingerprint and/or PIN.

Their biggest vulnerability is when an attacker uses a compromised credential to create approval fatigue. The attacker repeatedly initiates login attempts using the compromised credentials, triggering an out-of-band push notification on the victim's OOB mobile app. The constant barrage of notifications becomes annoying, leading the victim to improperly approve one of the login attempts, granting the attacker access to their account. To protect against this type of attack, these apps often require a response containing information in the push that forces the user to read the approval request. Besides being secure, mobile apps are simple and fast to use.

Push

- Enrollment process is typically self service
- Simple for user to approve

TOTP

- Confirmation isn't quite as quick because the user has to enter the token

Assurance strength **Usability** **Administrative overhead**

Proximity cards (what you have)

Proximity cards, commonly referred to as prox cards or key cards, work by NFC (near field communication) technology that wirelessly transmits data via an antenna to a card reader within a short distance. The data is read by a reader as code, usually a PIN, which is sent to the authentication system for verification. A chip embedded inside the card allows it to be quickly reprogrammed (activated, deactivated, changed) as needed.

Because they are so simple and fast to use, these cards are frequently used for:

- Physical access control: Building entry, restricted areas, parking garages
- Logical access control: Computer networks, secure applications
- Cashless payments: Public transportation, vending machines, cafeterias
- Loyalty programs: Membership identification, points tracking
- Time and attendance: Employee clocks in/out and tracks work hours

While prox cards are fast and simple, their security is limited. Since the data being transmitted isn't encrypted, it can be intercepted and thus cloned. They can also be stolen and have no way of verifying if their current holder is authorized. Because of this, prox cards are typically limited to physical access control points. For situations requiring a higher level of security, another method like biometrics or PIN is commonly added.

- Their inability to deliver nonrepudiation limits their use to specialized use cases where speed, efficiency, and simplicity are the dominant drivers.

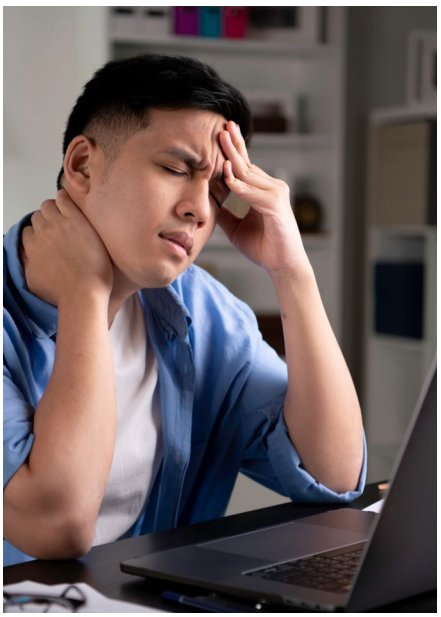
Smart cards (what you have and what you know)

Smart cards are also quite resistant to remote attacks, but they differ from proximity cards in that they use chips to transmit information rather than antennas. These chips vary in storage size and processing power, but all contain secure information (usually certificates). Smart cards contain secure microchips that encrypt sensitive data and perform cryptographic operations, so unlike prox cards, smart cards are highly resistant to tampering and malware attacks.

Smart cards are powered by the reader when inserted. It's at that moment that the certificate is verified. Depending on the use case, it's common to use a PIN to serve as another factor for sign in. While it's true that smart cards have the advantage of a secured form factor, they require a high-priced card management system. There is also a risk of the reader failing to read a chip, so it's also common to offer alternatives as authentication backups.

- Offers non-repudiation over prox cards
- Onboarding is more involved than prox cards
- Often used with a PIN, especially for remote identity verificationx

Assurance strength	Friction level	Administrative overhead



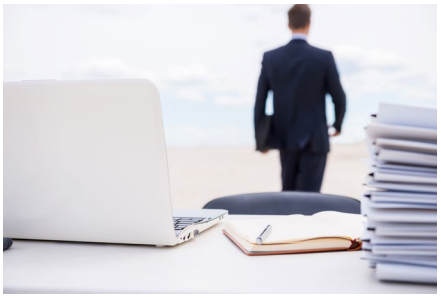
Challenge response/Knowledge-based authentication

Challenge response (also referred to as knowledge based) is one of the most requested non-cryptographic backup authentication methods. This method is a convenient fail safe for a user who might not have their primary authentication method available. Note that users must pre-enroll their challenge-response message pair prior to an attempted use.

Users allowed to log in with the challenge response (CR) method are presented with several pre-enrolled questions (the “challenge”) and they must provide valid answers (the “response”). This method is considered more secure than User ID and Password since multiple correct responses are required. As with any textual based process, challenge response is susceptible to eavesdropping and over-the-shoulder snooping.

In general, one of the goals of passwordless authentication is to balance security with user friendliness. The ideal identity verification system provides strong security while being easy and intuitive for users to navigate, this should also be a priority of CR. CR is often implemented as a backup journey when a different authentication fails. If the CR question(s) are difficult to remember or ask for things that can change over time (Eg. what is your age?), they could unnecessarily block a user from resolving their authentication issue.

- While onboarding is typically self-service, it is important for it to be with questions that can’t be researched online
- Spelling can be a problem, either with onboarding or responding
- Users may forget the response to the challenge question or change preference/habits



Bluetooth (passive)

Because of its flexibility and lower cost options, Bluetooth technology offers attractive options for authentication, especially when used as an additional layer of security as part of a multi-factor implementation, like GPS-based geofencing. As with the geofencing capability, the user can enroll their smartphone or a supported mobile device as theirs to create a “what I have” method. For example, if an organization wants to factor in their user’s proximity to their laptop, they are paired together as part of the enrollment process. The authentication agent on the laptop will alert the authentication infrastructure when the smartphone is out of Bluetooth range or disabled. This is the same perimeter model as geofencing, but it uses Bluetooth technology instead. As such, it is the same type of use case except that it’s about proximity to the device rather than a geo boundary.

Because of the real concern of someone close by taking a smartphone for quick access to a desktop or other secured device, when used on its own Bluetooth falls short of providing strong identity repudiation. Because of this, it’s more common to include Bluetooth as one of multiple authentication factors. So, Bluetooth (typically smartphone) can be used to signal that the user has moved away from the desktop or other environment. But more is needed to verify that it’s the user who has moved the device back within range.

- The rating below assumes Bluetooth on its own
- Access to sensitive information will typically require more than just Bluetooth.

Assurance strength	Friction level	Administrative overhead

Geofencing (passive)

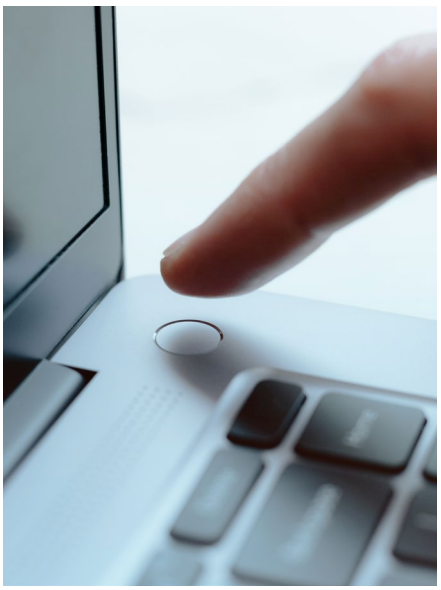
Geofencing is less of an authentication type and more of a way to gather information about where the user is located. Typical use cases consist of scenarios like users gaining simpler access when on campus than when off or is in an expected region rather than out of it. But geofencing can also serve as an authentication type in conjunction with another. This technology works especially well if a mobile out-of-band app includes geofencing to check whether the user is within an acceptable area.

While different location technologies are available, the most common is the Global Positioning System (GPS), which is a satellite-based navigation system. Smartphones commonly offer a GPS receiver capable of receiving signals from orbiting GPS satellites. The GPS coordinates gathered by the receiver can be captured by the mobile app to verify its location when an authentication request is received.

Biometric authentication methods

Biometric authentication verifies identity using unique physical or behavioral traits—such as fingerprints, facial features, or voice patterns. Unlike passwords or tokens, biometrics are inherently tied to the user, making them difficult to steal or replicate. This method offers high security with minimal user effort, enabling fast, intuitive access across devices and systems.

Assurance strength	Friction level	Administrative overhead



Fingerprint

Fingerprint authentication has become the most common passwordless authentication type. You often see it being deployed to unlock smartphones or secure mobile apps. This popularity stems from the fact that it's simple and secure. Fingerprints are highly resistant to phishing, which is the most common way credentials are compromised. Like other biometric and "what you have" authentication types, they're more secure in part before there is nothing to remember, and they can't be stolen. While biometric authentication types tend to be more expensive, fingerprint authentication systems can be implemented at a comparatively lower cost.

Although they interface like traditional fingerprint readers, vein readers authenticate users by scanning the unique pattern of veins beneath the skin, typically in the palm or finger, using near-infrared light. This light is absorbed by hemoglobin in the blood, allowing sensors to capture a detailed image of the vein layout. Because vein patterns are internal and require live blood flow to be read, they are nearly impossible to forge or replicate—offering a higher level of security than fingerprint readers.

Unlike a person's fingerprints, which can be damaged, worn, or lifted from surfaces, vein patterns remain consistent and are not left behind, reducing spoofing risk. Additionally, vein readers are more hygienic, often functioning contactless, and are effective even when skin is dirty, wet, or injured—making them ideal for high-security, high-traffic environments. Their superior anti-spoofing capabilities and reliability in various conditions make them a strong choice for organizations needing robust biometric authentication.

Regardless of the technology, users prefer fingerprint authentication because it's fast and convenient—their fingerprints are always on hand and readily accessible. With the adoption of fingerprint readers on smartphones, people are comfortable with them. The FIDO Alliance conducted a recent survey, finding that the majority of consumers prefer biometrics over traditional credentials.[1]

Beyond the traditional privacy concerns inherent with biometric authentication types, some users may have physical limitations that make it difficult to use fingerprint scanners. Obviously, for those users other methods will be needed.

- Dependency on the quality of device, which may be expensive
- Conditions of enrollment – onboarding process potential source of false identity (social fingerprint sharing)
- Devices need to be purchased and distributed to clients

Assurance strength	Friction level	Administrative overhead

1 FIDO Alliance, *2024 Online Authentication Barometer*, October 2024

Facial recognition

Today, facial recognition for passwordless authentication in the business world is still in its early phase. Aside from the dependence on hardware containing the right set of sensors, privacy concerns continue to limit its usage.

While laptop/desktop facial recognition for authentication is still fledgling, usage on mobile devices is more common. One key difference is that users typically own their smartphones, which reduces privacy concerns. They also seem more comfortable enrolling their face on their own smartphone than on a corporate device. Authentication scenarios that smartphone users are increasingly using facial recognition for include:

- Unlocking phone: The most common use of facial recognition on smartphones, offering a faster and more convenient method than passwords or PINs.
- Mobile money transactions: Some banking and payment apps support facial recognition for secure transactions.
- App authentication: A growing number of apps are offering facial recognition as an alternative login method.

While personal use of facial recognition for authentication is most common, adoption in the corporate sector is catching on. Today, the most common usage is:

- Access control: Securely granting employees access to buildings, restricted areas, or sensitive data.
- Time and attendance: Automating time tracking and attendance management.
- Fraud prevention: Preventing unauthorized access to systems and financial data.

While the adoption of facial recognition, obstacles remain for many organizations. While users may feel comfortable using facial recognition on their own devices, they may have concerns about potential privacy violations enrolling onto corporate devices. Other challenges an organization may face include:

Deployment cost and enrollment effort

For most environments, implementing facial recognition across an organization is more cost and effort than simple OTP. A segment of your install base may take a while to warm up to facial recognition, and some never may. There may be environments (combination of environment and hardware) that make it difficult to enroll a device. Potential obstacles include:

- Accuracy: Achieving consistently high accuracy can be a notable roadblock due to lighting variations, unusual poses, facial expression or angles, and low-resolution images or occlusions like sunglasses.
- Quality and diversity of datasets: One of the foremost challenges in training robust facial recognition models is the availability and quality of diverse datasets. Deep learning algorithms heavily rely on large and varied datasets to generalize well across different demographics, ethnicities, and environmental conditions. The users' willingness to properly or more effectively build (train) the dataset model will vary, resulting in varying levels of performance.

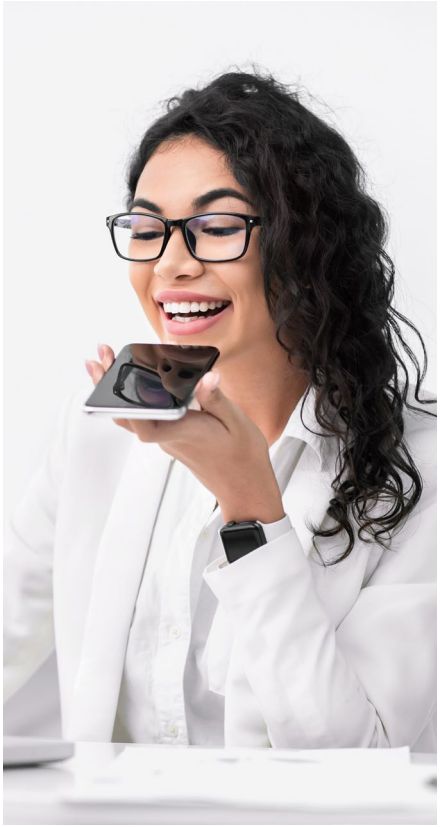
Cost

Hardware-based solutions (such as biometric devices) involve costs for purchasing, distributing, and maintaining devices. Software-based options have hidden costs like administration, migration, and ongoing maintenance.[1]

Since no authentication method is foolproof, it could make sense to add facial recognition's passive advantages as another method in a multi-factor authentication strategy.

- In large part, the assurance strength is dependent on the enrollment process
- Liveliness detection should be included as baseline
- Hardware and environment variability may degrade reliability and introduce friction
- Potential support from potential reliability issues

Assurance strength	Friction level	Administrative overhead



Voice recognition

Voice recognition is a method of verifying a person's identity based on their unique voice characteristics. Just like the other "something you are" methods already covered; voice recognition authentication offers higher security than passwords.

Like facial recognition, voices offer an advantage over fingerprint in that no surfaces need to be touched. Users who have challenges with their vision can still interact with their devices. This technology can capture speech faster than some users can type, improving authentication speed.

Unlike the other two biometric methods covered it will likely be important to offer alternative authentication options for voice recognition fails. Background noises and health conditions like colds or allergies can temporarily alter the user's voice. Another rapidly evolving risk is the quality and effectiveness of deepfakes, as well as the ability to identify them. This makes voice recognition limited in its application. For protecting highly sensitive information, voice recognition will have to be combined with another authentication type to meet security requirements.

Speech accents and homonyms—for example, see and sea—could result in increased input errors. As well, a voice recognition program runs many times faster if the entire vocabulary can be loaded into RAM compared to searching the hard drive for some of the matches. So processing speed is critical, as it affects how fast the computer can search the RAM for matches. Audio input needs to be analyzed for clarity, so some devices may filter out background noise.

Like the other biometric methods we covered, voice raises the same privacy concerns, requiring secure storage and ethical usage. With the emergence of generative artificial intelligence, which can imitate anyone's voice, scammers are using that technology to target people. AI-powered voice cloning can now mimic human speech with uncanny precision, injecting a potent dose of realism into phishing schemes.

- The accuracy of voice recognition quality (security) varies depending on the technology and algorithm
- Must be used in a quiet setting, which if not may introduce friction
- Human voice changes, compromising strength and reliability
- Often used in conjunction with another method such as PIN
- Identity verification is highly dependent on the enrollment process
- Vulnerable to deepfake voice reproduction.

Assurance strength **Friction level** **Administrative overhead**

Method management

As passwordless technologies continue to proliferate across various authentication use cases, the situations that need to be accounted for expand. With passwordless technology:

- Smartphone loss or damage would make SMS and agent-based methods inaccessible.
- Biometrics, such as fingerprint or face ID, may fail under certain conditions.
- A lost or malfunctioning hard token could block successful authentication.

As such, organizations need to provide secure enrollment for multiple authentication methods.

In B2C scenarios, businesses are increasingly allowing users to disable authentication types they are less comfortable with or feel are less secure. This level of flexibility and control gives the consumer more confidence in the security of the service, which may result in a higher level of trust.

As passwordless continues to extend into a more pervasive role across organizations, method management will take on an expanded role. Mature method management will be defined by the number of authentication types that are supported, the simplicity of enrolling them, and the level of control provided to be the administrators and users.

As cyberattacks grow increasingly sophisticated, finding the method that meets your requirements has the potential to grow more difficult. Yet, that balance is an important element when considering authentication methods. The wrong authentication type can be too cumbersome, hinder productivity, and drive users to circumvent policies, all of which erode trust in IT.

Enrollment process is a key factor

As you design your passwordless enrollment processes, it's critical to remember its role in the security and reliability of the method. Enrollment is the foundation where the user's identity is verified and securely bound to their authenticator—whether it's a biometric trait, device-bound credential, or cryptographic key. You must confirm that the individual is who they claim to be through rigorous identity proofing—either in person, remotely with identity documents, or via integration with existing verified identities. Once confirmed, the authenticator (e.g., fingerprint, passkey, security key) is cryptographically linked to the user's account. This secure binding ensures that only the rightful user can authenticate moving forward.

Wrap up

The more intuitive and seamless the authentication experience, the more likely users are to comply, reducing risky workarounds. Striking the right balance means designing security that protects the enterprise without becoming a barrier. You will likely find that both single sign-on and adaptive authentication are essential tools for reaching your goals.

Today's wide range of passwordless authentication options enables organizations to achieve the critical balance between usability and security—two goals often seen in tension. By leveraging technologies such as biometrics (fingerprint, face, voice), device-based passkeys, hardware tokens, mobile apps, and contextual factors like geolocation or device behavior, businesses can tailor authentication to fit risk levels, user roles, and interaction environments. It is hoped that this buyers guide accelerates your evaluation process as you look for technologies and solutions that fit your business model.

The breadth of passwordless solutions empowers organizations to implement authentication that is not only stronger, but smarter—raising identity assurance while creating a frictionless user experience that supports modern digital transformation.

What is passwordless authentication?

What is multi-factor authentication?

OpenText Advanced Authentication

opentext™