opentext™

An introduction to passwordless authentication methods

opentext™

Contents

opentext™

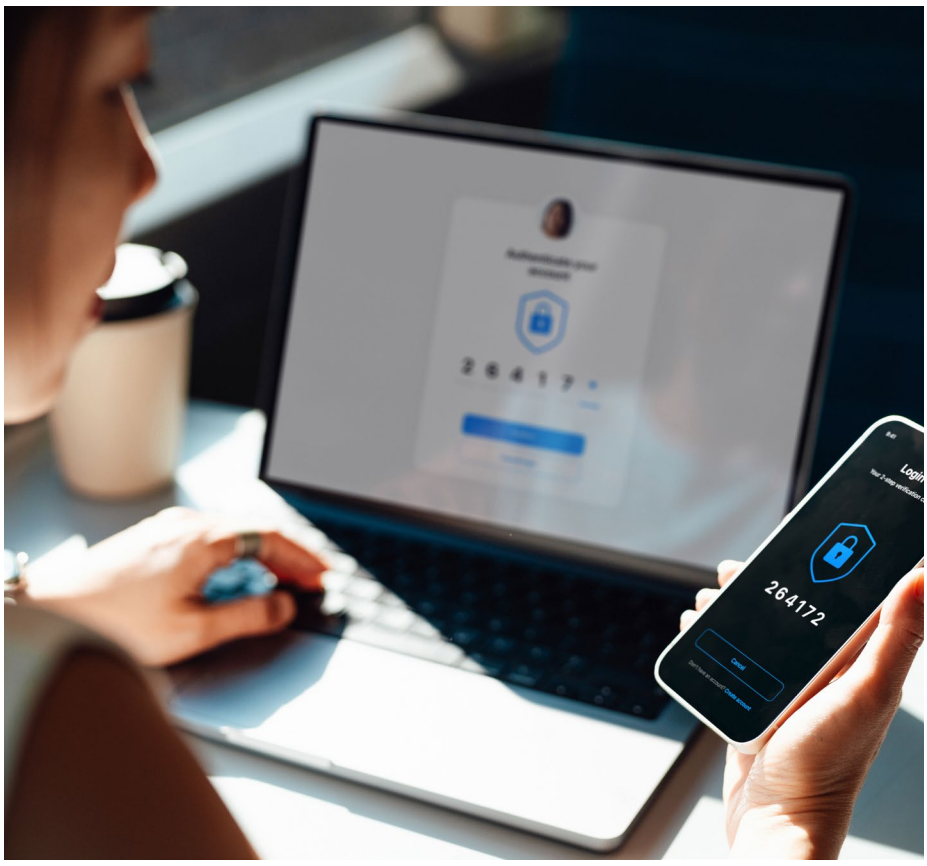
"2024 will be the year where we'll see real movement toward passwordless solutions, with demand for passwordless solutions growing at a faster rate than before."[1]

Executive summary

Authentication is the way organizations verify digital identities of both internal and external users. It's an essential part of an organization's security. Today, virtually every piece of information is created and stored digitally, and the digital world is both heavily distributed and connected. In this context, the need for passwordless technology to protect against malicious outsiders has never been higher.

Beyond increasing security, passwordless authentication can also simplify the authentication process by alleviating the burden of remembering credentials or typing them on small touchscreens. Fingerprint access, facial recognition, and other similar options make the process much easier.

Throughout this past decade, passwordless technologies have been needed to comply with government mandates requiring two-factor authentication. They continue to expand as organizations become more sophisticated in implementing risk-based multi-factor authentication. Biometric and passkey technologies are increasingly popular alternatives to traditional username and password implementations. This paper is intended to provide a solid resource to organizations that recognize they need to do more with strong authentication.



1 Beta News, Securing the world of tomorrow: Anticipating the IT security topics of 2024 and beyond, 2024

opentext™

Expanding your passwordless footprint

Passwords remain the de facto business credential because they are so easy to create and onboard. However, they are also easy to guess or steal through hacking, social engineering, or other strategies. Passwords are also often weak or reused across multiple accounts. Character-based credentials remain the primary target of malware and especially phishing attacks.

Compromised credentials remain the foundation of most data breaches. While no authentication method is perfectly secure, passwordless authentication credentials are much harder to phish, making them a significant improvement over traditional passwords.

Beyond security, passwordless authentication can also be more convenient and flexible. It eliminates the need to remember and manage multiple passwords for different accounts. Instead, users can verify their identity using a single authentication factor, such as their fingerprint or a security key. Access can be further streamlined with single sign-on strategies.

Passwordless authentication is also typically faster and simpler than traditional credentials. Depending on the method, users can access systems, services, devices, and other resources with a single tap or click.

Evaluating methods

Below is a list of suggested criteria for selecting authentication types or the devices that enable the authentication flow. Because each organization has its own environment and set of priorities, this paper is intended as an aid for decision makers and influencers rather than a simple selection formula.

User requirements

While the office environment is relatively easy to secure, worldwide trends show a movement to professionals working remotely at least some of the time.[2] These remote situations often present challenges to keeping access to sensitive information both simple and secure. What devices may be available and whether the user is in a remote office, out in the field under potentially diverse conditions, or traveling, may likely need to be accounted for.

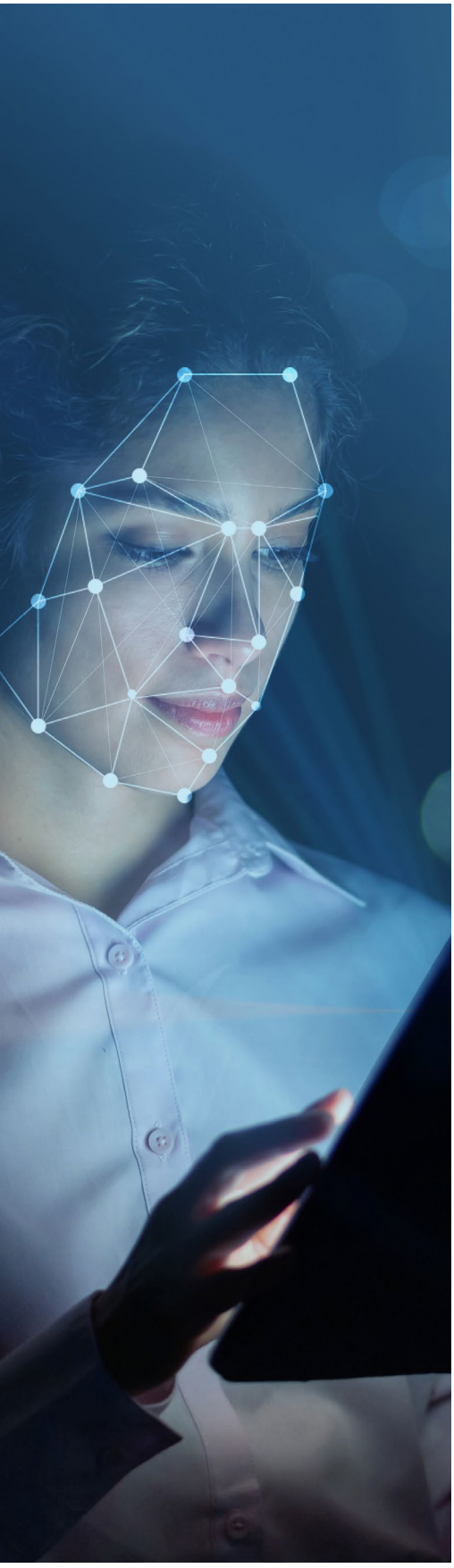
Investment and cost

While licensing, as well as shipping, handling, and vendor support fees, are always top of mind when measuring costs, other factors can prove even more expensive.

Here are some common cost points:

- **Deployment costs**
  These include the costs of configuring and distributing physical devices to users and training users on how to use them. Typically, physical methods, such as hard tokens, have higher deployment and logistics costs, especially for organizations with users who are geographically dispersed.

2 Werc, Adapting to the New World of Work: Remote Work Trends Across Global Reasons, 2023



- **Maintenance**
  Devices that must be physically assigned by an administrator, either in deployment, replacement, or troubleshooting, are expensive and not very scalable. Some organizations still choose these high-touch devices because they meet their security and physical requirements. An ideal approach may be to have one authentication type for high-risk users and others for the rest of the organization. Drive down maintenance costs by establishing a central point of administration for top-down template and policy management and then implementing self-service so users can manage their own accounts.
- **Soft costs**
  Although they are hard to quantify, soft costs are real. They are measured in metrics like lost productivity due to unreliable or cumbersome authentication. Because each organization is unique, you'll have to target the value of each of your top business processes and determine lost value complex access imposes on them. In the case of B2C interactions, a common symptom of credential barriers is consumers abandoning a transaction or interaction after multiple tries.

User acceptance and potential resistance

There are two levels of resistance to the adoption of new authentication methods:

1. At the management or sponsor level, there is often a lack of awareness of the benefits that passwordless methods yield, such as improved security and convenience.
2. At the user level, fear of change or hesitancy to incorporate the unfamiliar is common. Some worry that a new passwordless option would be more time-consuming than sticking with traditional credentials.

The most common misstep, and hardest to recover from, is incorporating methods that slow down business for employees or drive away customers. A smart safeguard against failed deployment is ensuring that the new technology is at least as convenient as what it is replacing.

For example, if you already offer one-time PIN (OTP), out-of-band push is a natural extension that many people will prefer over typing in PINs. Others might prefer using fingerprint scanners over OTP options, which are common on phones and increasingly found on laptops.

It's best to add to rather than replace methods. If you are forced to remove a method, it is beneficial to provide users with long lead times that allow them to try other methods with their existing one as a backup until it's phased out. During this lead time, it is important to constantly monitor the adoption rate with the support of enrollment and authentication reports.

Recovery and other support

Credentials should never block an authorized user from doing their job or a consumer from engaging in an interaction. There must be a process in place for users to perform actions such as resetting a PIN, getting an updated certificate, or replacing verified devices. Having alternative methods of authentication available for users during "exception scenarios" is also a good practice.

Security

Beyond usability, methods must be assessed for their ability to protect against threats, including phishing, malware, and social engineering. To deliver the right level of identity verification, some methods may be considered a good fit for low-risk resources but not for higher risk ones.

Security teams must conduct ongoing evaluations of different methods in various situations. It's possible to improperly implement a method, undermining its security. Practices can become the weak link that compromise the administration's security, ongoing governance, and enforcement. They must be verified and periodically reviewed, with exception cases reconsidered.

Authentication types and considerations

The passwordless authentication market revenue is estimated to reach more than $20B in 2024 and is expected to double within the next five years.[3] As this demand drives rapid change, any comprehensive guide to authentication method options is quickly outdated. This paper is intended to serve as a foundation for further research rather than an exhaustive list.

It's important to remember that your user base may need to authenticate under various situations and with different devices. The more options you're reasonably able to offer, the more likely a user will have access to one that best fts their needs.

In their quest to protect themselves against increasingly sophisticated attacks, organizations are transitioning to methods that continuously evaluate risk and user behavior to determine authentication needs. The more passive or low-friction methods you have available in your environment, the more convenient it will be for your users who may need to verify themselves multiple times during a session. Passive authentication options allow your security infrastructure to re-verify a user's claimed identity without disrupting the user.

Traditional username and password

From their initial experience with digital devices and services, users are taught to verify their identity with a username and password. Usernames and passwords will continue to be an authentication mainstay for the foreseeable future because they are simple and, more importantly, very familiar.

One of the strongest forces backing traditional credentials is that virtually every platform, application, and service supports them by default. This drops initial investment requirements substantially because there is no need to invest in specialized hardware or software and the infrastructure. This default infrastructure is typically highly scalable, making it a safe choice for large organizations and enterprises.

3 Statista, Passwordless authentication market revenue worldwide from 2021 to 2030, 2024

opentext™

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 displayed at the moment they need to respond to an authentication challenge.

As a variation, OATH (Open authentication)-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 due to their open-standard 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 deliver strong security, usability, and overhead costs have limited their use:

- Enrollment is a hands-on process that requires an administrator to manually assign a device to a user and then send it to them.
- When a token requires support or troubleshooting, it may likely involve the user sending the device back to central IT.

Since the use of multi-factor authentication is far more pervasive now than when hard tokens were adopted, other authentication types may need to be deployed across the organization to control costs and administrative overhead.

opentext™

Remote situations often present unique challenges to keeping access both simple and secure.

Mobile SMS: One-time PIN

Today, short message service (SMS) OTP is the most common type of second factor authentication. It's popular because most individuals performing transactions own a mobile device and are familiar with SMS, making it a simple and familiar action. It capitalizes on the fact that people usually keep their phones with them.

Three foundation points to the SMS-based OTP security model are:

- The owner's identity was verified when it was assigned to a specific SIM (subscriber identity module) card or built-in eSIM, which are tied to a phone number.
- The OTP is separate and 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, one-time PINs (TOTP). Once the PIN's lifespan has expired, they are worthless for confirming one's identity.

While mobile SMS-based OTPs deliver strong security, they do have vulnerabilities. A man in-the-middle scenario poses a threat, since it is possible to intercept SMS messages, potentially exposing your OTP. SIM swapping is another risk, and social engineering is still possible.

Out-of-band push to mobile app

Out-of-band push mobile app authentication differs from SMS in that a specific mobile app, not a phone number, is tied to the primary identity provider (IdP). Like SMS, these out of-band mobile apps typically push 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, this method yields a higher level of security. Additionally, in most situations, approving a push notification is faster and more convenient than typing in a PIN.

However, this method is not immune to attack. While notification encryption secures the messages, if the user's device is compromised or stolen, an attacker may be able to approve fraudulent authentication attempts. Additionally, users may become accustomed to approving requests without thoroughly verifying their legitimacy.

Proximity cards

Proximity cards, commonly referred to as prox cards or key cards, work by wirelessly transmitting 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 clock-in/out, tracking 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 reserved for payment systems and physical access control points. For situations requiring a higher level of security, another method like biometrics or PIN is commonly added.

Smartcards

Smartcards contain secure microchips that encrypt sensitive data and perform cryptographic operations, so unlike prox cards, they are highly resistant to tampering and malware attacks. These chips vary in storage size and processing power, but all contain secure information (usually certificates).

The smartcard is powered by inserting it into the reader. At that point, the certificate is verified, often with a PIN to serve as another factor for sign-in. One disadvantage of these more secure cards is that they require a high-priced management system.

Fingerprint

Fingerprint authentication has become the most common passwordless authentication type in use. You often see it being deployed for unlocking smartphones or secure mobile apps. Since fingerprint delivers superior speed and convenience, their usage exceeds both OTP and facial recognition.

Biometric authentication, such as fingerprint, is attractive to many organizations because:

- It solves the problem of users needing to remember multiple credentials and all the problems users create when they try to manage that challenge.
- They're unique and difficult to forge.
- They're generally faster than typing passwords, making for a smoother user experience.

Since there have been instances where hackers have been able to bypass fingerprint authentication, care should be taken to determine whether they meet your security needs. In your determination, remember that not all smartphone readers use the same technology (capacitive, optical, ultrasonic), which may force organizations to limit their use to multi-factor authentication, especially for mobile BYODs (bring your own device).

While fingerprint authentication has many advantages, use cases that exclude mobile devices bump up against cost and rollout logistics. Extending fingerprint authentication to laptops and tablets is more difficult. Today, with a growing market size that today is more than $3.5B,[4] fingerprint readers are becoming common on electronic devices, including laptops. This means that adopting fingerprints will require purchasing new hardware devices (either laptops or FIDO readers).

Facial recognition

Facial recognition for passwordless authentication in business 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 fledgling, usage on mobile devices is much more common. One key difference is that users typically own their smartphones, which reduces privacy concerns as users seem more comfortable enrolling their face on their own device than a corporate one.

Smartphone users are increasingly using facial recognition for authentication scenarios such as:

- **Unlocking phones**—the most common use of facial recognition.
- **Mobile money transactions**—some banking and payment apps support facial recognition.
- **App authentication**—a growing number of apps include facial recognition as an alternative log-in method.

Adoption in the corporate sector is slowly catching on, with the most common applications being:

- **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 by including user verification and validation against national identification databases.

4 Markets and Markets, Fingerprint Sensors Market Size, Industry Report, Trends, Growth Drivers, Opportunities, 2030

Challenge response/knowledge-based authentication

Challenge response (also referred to as knowledge-based) login 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. It's important to note that this method only works if users pre-enroll their challenge-response message pair prior to an attempted use.

Users allowed to log in with the challenge response 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. However, as with any textual based process, challenge response is susceptible to eavesdropping and over-the-shoulder snooping.

Geofencing (passive)

So far, the authentication types discussed impose some level of user friction; meaning that users must perform an action to verify their identity. While biometric authentication options are low friction, they do interrupt the user in high security situations, where continuous authentication is active throughout the session. Passive authentication affords the benefit of verifying the user's identity without any action.

Geofencing is the use of location technology as a datapoint confirming an authenticated identity. For example, if an employee was in the office or corporate campus when authenticating onto the intranet, geofencing technology can be used to confirm that the employee is indeed on site.

While different location technologies are available, the most used is the Global Positioning System (GPS), which is a satellite-based navigation system. Smartphones commonly include a GPS receiver and the coordinates it gathers can be captured by a mobile app to verify its location.

As a passive authentication type, geofencing is well suited as a second factor for multi-factor authentication. However, it can be time-consuming to decide and define possible "allowed" locations where the user can authenticate. Even so, for mobile users, geofencing can be helpful in determining the strength of authentication that is appropriate.

Bluetooth (passive)

Bluetooth technology can be used in a similar fashion to geofencing, but is instead sensing proximity to the device rather than a geo boundary. The user enrolls their supported Bluetooth device, for example, pairing a laptop with their smartphone. The authentication agent on the laptop will alert the authentication infrastructure when the smartphone is out of Bluetooth range or disabled. For example, if a user walks out of the office leaving the Bluetooth enabled workstation, the workstation can lock automatically when the user's phone is out of range.

Voice recognition

Voice recognition authentication is a method of verifying a person's identity based on their unique voice characteristics. It's another form of biometric authentication with similar benefits. Just like the other "something you are" methods, voice recognition authentication yields higher security than passwords. There's nothing for the user to forget and voices are also phishing resistant.

Like facial recognition, voices have intrinsic advantages over fingerprint in that no surfaces need to be touched. Unlike the other two biometric methods covered, it will likely be important to offer alternative authentication options in case voice recognition fails. Background noises and health conditions like colds or allergies can temporarily alter the user's voice.

The use of AI to create fake voice prints exposes another limitation of voice recognition systems. If your organization uses voice recognition, they may find it necessary to add another method, such as "something you know," to use along with it. Like the other biometric methods we covered, voice also raises privacy concerns, requiring secure storage and ethical usage.

Standardized authentication interfaces

Beyond the methods themselves, the authentication interfaces and standards listed below offer a practical approach to implementing a robust and user-friendly passwordless environment. They're the best route for achieving a cost-efficient framework capable of protecting a wide variety of applications under a broad set of user requirements and situations.

RADIUS

While designed for authenticating remote dial-in users, today RADIUS (Remote Authentication Dial-In User Service) is a common integration point for web and internal applications and services that don't directly support modern protocols like OpenID Connect and SAML.

Authentication management vendors often rely on RADIUS to provide compatibility to authentication types that they don't support natively. It can act as a centralized gatekeeper (important for organizations centralizing authentication administration) for identity verification but can also contain authorization information.

FIDO Alliance

The FIDO Alliance is an open industry association formed to reduce the world's reliance on passwords for online authentication. Its strategy is to develop and promote standards for strong authentication. The organization has support and cooperation from 250 key vendors, including the likes of Google®, Microsoft®, Apple®, and Samsung®. The FIDO Alliance estimates that there are four billion FIDO enabled devices in use.

FIDO Universal 2nd-Factor (U2F)

U2F was designed to support external hardware security keys to support two-factor authentication (2FA). These keys, typically USB or NFC-based, store cryptographic keys specific to each online service. During log-in, after entering traditional credentials, the user touches the security key to complete the 2FA process and grant access.

In 2018, the FIDO Alliance updated the U2F use case with Client to Authenticator Protocol (CTAP) to directly support passwordless authentication scenarios. This newer protocol allows users to log in to websites and apps without using passwords at all, relying solely on biometrics or security keys. Both protocols deliver high security even though CTAP offers enhanced security over U2F.

FIDO Universal Authentication Framework (UAF) and FIDO2

UAF was designed to support the FIDO ecosystem for achieving passwordless authentication. It focuses on leveraging FIDO devices' built-in security features, such as biometrics (fingerprint, facial recognition), PINs, or security keys to authenticate to online services instead of traditional passwords. Overall, FIDO UAF played a crucial role in introducing passwordless authentication and paved the way for the more advanced FIDO2 technologies.

While it remains a viable option for secure logins, especially if compatibility with older systems is a concern, FIDO2 extends it to signing transactions and verifying assertions. UAF uses browser-based protocols, while FIDO2 uses platform-specific APIs for increased security. As such, today FIDO2 is the preferred approach for new implementations due to its broader capabilities and security enhancements.

Summary

With careful planning, early leader engagement, and phased implementation, passwordless authentication can help to make your organization more secure and efficient internally while enhancing digital engagement with your consumers.

Because passwords are inherently vulnerable to hacking, phishing, and brute-force attacks, passwordless authentication offers a significant step forward in securing sensitive and regulated information. While no authentication is 100-percent foolproof, not only are biometric and cryptographic keys much more secure than traditional credentials, but they are also simpler and far speedier. Overall, passwordless authentication removes the struggles of users trying to remember and manage their claim ID and accompanying complex passwords. It is hoped that this paper will spur your organization on its journey to a new passwordless environment or to making your existing password environment more secure.

For information on OpenText's authentication solutions, check out the NetIQ Unplugged channel on YouTube.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- X (formerly Twitter) | LinkedIn