Tech Brief

SecureDoc by WinMagic

PASSWORDLESS AUTHENTICATION
– A technical viewpoint

Passwordless authentication is set to resolve many issues of traditional passwords, including operational, usability, and security challenges. However, most passwordless solutions have gaps, and achieving a fully passwordless future remains a long journey.

Passwordless authentication today

Challenge of passwords
With username and password authentication, you must remember many long passwords, one for each server or website. Using the same password for multiple sites poses a security risk, as a breach at one site can compromise others.

Workarounds with password managers
To address this, password managers store many long and complex passwords in a secure vault on your device or in the cloud, reducing the need to remember each one individually.

Risks of identity theft
Identity theft remains a growing threat. Even with a secure device and a password manager, passwords can be stolen through phishing and man-in-the-middle attacks. Since passwords are static, they can be reused by attackers. A solution to this issue is adding a dynamic factor, such as a One-Time Password (OTP) token or SMS message. These temporary passwords, typically six-digit PINs, change with each use and cannot be reused, enabling multi-factor authentication (MFA).

Vulnerabilities of OTP and SMS
Despite being dynamic, OTP and SMS have their vulnerabilities:

SIM swapping attacks
Attackers can convince your carrier to switch your phone number to a SIM card they control, allowing them to intercept your SMS messages.

Shared secret vulnerability
Since OTP is based on a shared secret, it is susceptible to server-side attacks like password authentication.

Inconvenience of physical factors
The additional physical factor required for OTP or hardware tokens can be inconvenient. Not everyone wants to install a company-approved OTP authentication app on their phone, nor do they want to carry an extra hardware token, which can be lost and needs replacement.

Complications with passwordless authentication

Passwordless authentication aims to resolve password-related issues by preventing data breaches caused by credential and identity theft through phishing and malware attacks. This approach has led to a growing adoption of passwordless methods among security professionals and organizations. However, passwordless authentication has its complications that need to be addressed:

Hardware tokens
- Passwordless authentication can be implemented with hardware tokens but shares similar issues with OTP hardware tokens.
- Users must carry an extra item, and companies must manage these tokens, including buying, tracking, distributing, and replacing them if lost.
- Often, two tokens are issued per user to prevent lockouts, adding to the overhead problem.

Mobile push
- Using a phone for passwordless authentication, known as “Mobile Push,” has issues similar to an OTP mobile app.
- Companies may need to buy expensive phones for users or take control of personal phones, which employees might resist.
- Security risks include users inadvertently accepting “push” attacks.

WinMagic standards and advancements for non-Web applications (like VPN, legacy, and rich-client applications) provide more effective solutions than other options on the market.

SecureDoc by WinMagic

"Passwordless" Authentication

a. 006092

Passwordless: No centrally managed passwords.

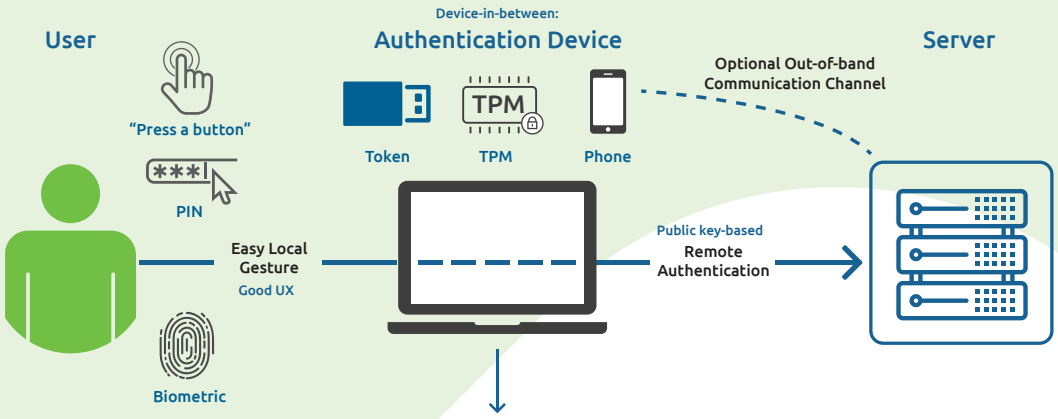

Figure 1

The authentication device in-between performs strong authentication to the remote server. Without possession of the authentication device - the private key - no one can login as this user!

Simplifying authentication without risking security

Business users want to work on their primary devices without the hassle of extra factors like phones or hardware tokens. The device they're on — a laptop, Mac, or phone — can be the second factor for secure authentication. Here's how:

Device as MFA

- No need for extra tokens or phone fiddling.
- The computer itself logs users into remote servers.
- Users provide a "local gesture" (e.g., biometrics, a short PIN, pressing <Enter>, or nothing) to confirm login.
- WinMagic simplifies this process with our software technology.

MFA at pre-boot and beyond

Local device login

- MFA is crucial when logging into the computer.
- Not typically part of the "passwordless" movement but should be considered.
- WinMagic offers unique MFA for pre-boot authentication.

WinMagic's SecureDoc pre-boot

- Manages authentication/access to BitLocker-encrypted devices and Self-Encrypting Drives.
- Supports MFA options like YubiKey token, PIV, and smartcards.
- The only vendor currently offering MFA at pre-boot.

Transition to Passwordless Authentication

Server/application side changes

- Shift from username and password to passwordless authentication.
- WinMagic helps identify which applications to start with, considering usage frequency and early adoption of passwordless solutions.

Industry support

- Companies like Microsoft, Google, and Apple back FIDO, the leading passwordless authentication standard.
- Increasing support for passwordless remote apps.
- Enables phasing out OTP hardware tokens and phone apps.

Understanding passwordless authentication

Passwordless authentication allows the server to verify a user without relying on shared secrets, such as passwords. Instead of storing or sharing passwords, the user authenticates locally on their device with a PIN, biometric data, hardware token, or a mobile phone. The device, not the user, then authenticates to the server using public key cryptography, proving possession of the private key without transmitting the PIN or biometric data.

WinMagic, a member of the FIDO Alliance, supports this method. The FIDO Alliance is dedicated to developing authentication standards that reduce reliance on passwords by using public key cryptography for stronger, phishing-resistant authentication.

fido ALLIANCE

SecureDoc by WinMagic

5 steps toward a passwordless journey

1. Transition to public key-based authentication for Windows login

Switching Windows logon to public key-based authentication marks a significant shift in the passwordless era. Here, authentication over the network moves from "username and password" to public key-based methods, ensuring that attackers cannot log in without the MFA factor, even if user passwords are stolen via phishing.

Configuration Needs:

- Enterprises must configure AD or Entra ID for strong authentication.
- Endpoints require MFA, and WinMagic's software tokens eliminate the need for costly hardware tokens or phone apps.

2. Secure Entra ID and implement MFA for endpoints

Once Microsoft Entra ID authentication is secure, other applications relying on Windows logon, like Outlook, Office 365, and Windows Remote Desktop, will also be secure. While some integration work may be required, the move toward passwordless authentication will eventually encompass most enterprise applications.

3. Secure applications relying on Windows login

With Entra ID as the authentication server and WinMagic MFA tokens on endpoints, enterprises can transition to passwordless authentication. VPNs and other applications are already adopting this method. Passwordless authentication will soon be a plug-and-play solution for many popular applications when using Entra ID or another server. The authentication server and endpoint client will manage most applications seamlessly.

4. Adopt passwordless authentication for enterprise applications

WinMagic's authentication client is designed for ease of deployment and flexibility, offering:

Comprehensive options:

- **Software token**
- **TPM**
- **PIV card**
- **FIDO token**
- **Phone**
- **Various combinations**

WinMagic's endpoint solutions offer flexible "local gesture" options, such as "PIN + biometrics" or "no PIN + monitoring device-level signals."

The PC is best for user authentication

Public key cryptography makes the PC with the TPM the most secure second factor in MFA, whether used alone or with another MFA factor.

5. Leverage WinMagic's comprehensive authentication solutions

SecureDoc FDE offers unique multi-factor authentication at pre-boot and secure single sign-on (SSO). This enables seamless integration with passwordless authentication for remote sites and services once in Windows.

Interested in learning more about how to ease into your passwordless authentication journey from WinMagic? Contact sales at sales@winmagic.com

US & Canada +1 888 879 5879 | EMEA +49 69 175 370 530 | Japan +03 5403 6950
For more information, click here or contact WinMagic

WINMAGIC