Tech Brief

# Passwordless Authentication for Air Gapped Networks

## Challenge/ Situation

Some organizations must operate their systems air gapped from the rest of the world for security and compliance reasons. Examples include classified government networks and sensitive financial and critical industrial control systems. This means no connection to external networks is allowed, especially the Internet. In many cases, mobile phone authenticator apps are not an option because the users are not allowed to bring their phone into the facility. They need secure Windows logon and SSO (single sign-on) to the many specialized Service Providers (SPs) on the enclaved network. Still, the leading IAM (Identify Access Management) SSO solutions are not an option because they are often provided as SaaS.

In addition, some government agencies may require PIV cards as the user authentication method.

## Solution

WinMagic supports several options for Windows logon (and PBA logon for full disk encrypted) systems, including:

- Trusted Platform Module/ Personal Identification Number (TPM/PIN)
- Smartcard/Personal Identity Verification Cards (PIV) for MFA
- Yubikey for MFA

Mobile phones are not required, but if they are allowed as long as they remain air-gapped, then Passwordless Phone Authenticator via Bluetooth Low Energy (BLE) could be an option.

Once logged into Windows, MagicEndpoint executes. MagicEndpoint consists of two main components:

1. The MagicEndpoint Client software that runs on the Windows machine
2. The MagicEndpoint IdP software that runs on a Windows server

MagicEndpoint IdP can be deployed on-premise by the organization and need only be connected to the air-gapped network, and no external network connections are required.

Regardless of the method for Windows Logon authentication, the MagicEndpoint Client software creates a unique public / private key pair for each user/device combination. The private key is protected in hardware by the device's TPM (Trusted Platform Module). The keys are non-duplicable.

# Windows Login

MagicEndpoint allows organizations to enable Windows login by providing the tools to easily deploy and use authentication that best suits their users.

Here is a summary of our solutions:

## TPM/PIN Use Case:

The TPM hardware on the device itself is a good option for organizations that find external tokens and devices hard to manage. Users log into Windows using the TPM with a local PIN, and Windows Login is protected by the TPM and can be configured for SSO. The TPM PIN is local and cannot be attacked remotely, and TPM also provides hardware-based anti-hammering protection.

## PIV Card Use Case:

For organizations mandated to use PIV Cards for access control, users access Windows using their PIV card. Windows Login is protected by the PIV card and can be configured for SSO for the best user experience.

## Passwordless Phone Authenticator via Bluetooth Low Energy (BLE)

For organizations that issue phones to employees and prefer this device for authentication, the MagicEndpoint BLE (Bluetooth Low Energy) mobile phone authenticator is a good choice. Unlike Out of Band (OOB) mobile authenticators, the BLE mobile authenticator communicates locally to the endpoint device and requires proximity to work. This proximity provides a strong association between the authenticator and the endpoint. MagicEndpoint phone-based authenticator authenticates to the laptop via Bluetooth to give the high-assurance, cryptographically enforced, MFA Passwordless login to the endpoint.

Users don't have to enter anything on the endpoint for a truly passwordless experience, and no external network connection is required.

These same methods can be employed for PBA login, too if you are using FDE, providing a consistent user experience. Once the user is authenticated to the endpoint, MagicEndpoint can provide "no user action" authentication to remote services on the air-gapped network seamlessly.

**MagicEndpoint from WinMagic is the passwordless authentication solution that protects access by focusing on the endpoint, for the user. It requires no user action, and no third-party devices or keys, so it's seamless, secure and virtually invisible.**



US & Canada +1 888 879 5879 | EMEA +49 69 175 370 530 | Japan +03 5403 6950

For more information, click here or contact WinMagic