Accelerate your Zero Trust journey

Recognized as global leaders in cybersecurity and delivering solutions purpose-built to bring their customers to Zero Trust, Yubico and Microsoft are FIDO Alliance members committed to providing phishing-resistant authentication solutions based on FIDO2 and certificate-based authentication standards.

Reference these use cases to understand how your organization, whether public or private sector, can block any sign-in attempt that does not use CBA and ensure your users are protected by leveraging secure, phishing-resistant, multi-factor authentication solutions with a passkey.

Certificate-based Authentication (CBA)

**Use cases**: Mobile restricted environments, shared workstations

**Industry**: Federal government and enterprises that interact with federal governments

CBA enables organizations with existing smart card and public-key-infrastructure (PKI) deployments to authenticate to Microsoft Entra ID (formerly Azure AD) without a federated server.

Use the same YubiKey as a smart card with Entra ID enabling you to migrate away from on-premises authentication solutions like ADFS as part of your Zero Trust and cloud strategies.

CBA on iOS and Android for federal government and enterprises

**Use cases**: remote workforce

**Industry**: Federal government and enterprises that interact with federal governments

Provides users with the same convenient smart card authentication method on mobile devices that they have on their desktops.

CBA has been a staple of governments and high security environments for decades, long before the invention of FIDO U2F and FIDO2, mostly due to its reliability and effectiveness in physical environments.

The YubiKey is currently the only external device that supports CBA on Android and iOS. Plus, the YubiKey is the only FIPS-certified, phishing-resistant solution available for Entra ID on mobile.

“As the threat of sophisticated cyberattacks continues to rise, ensuring our customers have access to phishing-resistant MFA methods like YubiKeys while using our products and platforms is critical. Thanks to our collaboration with Yubico, we’re thrilled that our federal government and enterprise customers can now use Entra ID CBA on iOS and Android devices to comply with the Executive Order on improving the Nation’s Cybersecurity that directs the use of phishing-resistant MFA on all device platforms.”

Natee Pretikul | Principal Product Management Lead | Microsoft Security division
Conditional Access
Authentication Strengths: Enforced FIDO or CBA

**Use cases:** All. Remote workforce, privileged access, mobile restricted environments, shared workstations

**Industries:** All including Public Sector, Retail & Hospitality, Manufacturing, Financial services, Healthcare, Cyber insurance, Telecoms, and more.

Fight phishing attacks by implementing specific user authentication policies. Leverage YubiKeys for phishing-resistant MFA for FIDO-based passwordless (FIDO2/WebAuthn) or CBA to enforce that YubiKeys are the only authentication solution allowed.

Restrict authentication to an organization's requirements. Eliminate an entire attack vector for your most privileged users and safeguard your most critical assets by configuring Entra ID to require YubiKeys for phishing-resistant authentication.

Azure Virtual Desktop (AVD) and Remote Desktop adds support for FIDO authenticators

**Use cases:** Remote workforce, privileged access

**Industries:** All including Public Sector, Retail & Hospitality, Manufacturing, Financial services, Healthcare, Cyber insurance, Telecoms, and more.

Connect to a personal workstation in the cloud with the same security and work experience no matter where you are.

FIDO-based passwordless authentication in AVD enables users to authenticate with their YubiKey and Entra ID passwordless credentials when the user signs into AVD or when they sign into an application inside their virtual desktop.

Passwordless authentication

**Use cases:** All. Remote workforce, privileged access, mobile restricted environments, shared workstations, consumers

**Industries:** All including Public Sector, Retail & Hospitality, Manufacturing, Financial services, Healthcare, Cyber insurance, Telecoms, and more.

Login without a password using phishing-resistant FIDO2 authentication.

Login to Windows 10/11 workstations, native apps, web applications and remote desktops with a FIDO2 YubiKey.

Learn more about how Yubico and Microsoft are stronger together

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy with phishing-resistant MFA. Yubico is setting global standards for secure access to computers, mobile devices, and more, and is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: [www.yubico.com](http://www.yubico.com).

© 2023 Yubico