A dedicated technical engagement designed to help you implement YubiKeys and MFA with Microsoft Azure AD Hybrid using Certificate-Based Authentication (CBA).

Yubico is leading the charge toward a more secure and frictionless authentication future. Our team of accredited security experts offers unique guidance and expertise in a comprehensive and targeted project designed to help you quickly and easily integrate YubiKeys with Microsoft’s MFA and passwordless functionalities in the Azure AD environment.

Professional Services offers a targeted two-week engagement designed to assist you in:

- Enabling your Azure AD passwordless environment
- Establishing your Azure AD hybrid join for domain machines
- Configuring Smart Card protocol for your privileged users
- Reviewing Remote Desktop MFA and other use cases, including Virtual Private Networking (VPN)
- Applying YubiKey lifecycle management and implementation best practices

Benefits include:

- Enhanced security through implementing strong authentication throughout your organization
- Enabling Certificate-Based Authentication (CBA) for Windows logon, cloud application and mobile devices
- Enabling on-premises Smart Card (PIV) passwordless logon for your privileged domain users
- Allowing convenient and secure Single Sign On or passwordless authentication for your Remote Desktop environment
- Review of options for securing your VPN access

Includes 20 hours of post-integration Professional Services assistance

For more information, go to Yubico Professional Services or contact your Yubico Sales today.

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also 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.

Professional Services
Microsoft Azure
CBA Implementation

Topics Covered
Our Professional Services team will cover these topics in your engagement:

Use Case Review
- Examine your technical architecture and use cases to ensure the optimal fit

Certificate-Based Authentication (CBA)
- Enable CBA in Azure AD
- Test CBA with cloud applications
- Test CBA with Windows logon (optional)
- Test CBA with mobile devices (optional)
- Configure Authentication Strength Policies (optional)
- Configure Conditional Access Policies (optional)

On-premises Smart card (PIV implementation)
- Discuss fundamental PKI concepts and assist in reviewing/standing up your PKI environment.
- Configure your Certificate Authority (CA) for self-enrollment and deploy the YubiKey minidriver and YubiKey Manager.
- Review smart card PIN change, PIN reset (PUK), as well as auto enrollment, enroll-on-behalf and self enrollment.
- Discuss Key removal behavior (lock/logoff) and smart card enforcement

Operational deployment best practices

Who should attend:

- Network/infrastructure admins that maintain Windows domain, servers and workstations
- Cloud administrators responsible for Azure AD/365
- Web administrators (for making certificate revocation list publicly-accessible)
- Deployment project managers

Includes 20 hours of post-integration Professional Services assistance