yubico

New tools to prevent phishing with Azure AD and YubiKeys Q&A

Q: Does CBA and FIDO work with a federated ADFS tenant?
A: ADFS has long-maintained native features to support smart cards and certificate based authentication. Those features are still supported today and can be used with YubiKeys. The new Azure AD CBA features allow sign-in with CBA without ADFS. ADFS itself does not support FIDO2 authentication however a tenant federated with ADFS can still leverage FIDO2 passwordless authentication using the Azure AD capabilities.

Q: Is MS Entra used to replace ADFS?
A: Entra with Azure Active Directory may be used to replace the capabilities of ADFS. With Azure AD CBA, organizations can either migrate a subset of their users with a phased rollout approach or optionally rollout for all their users. Organizations should review their requirements to ensure that Azure AD capabilities will replace all the capabilities that they are currently leveraging in ADFS. Please see Migrate from federation to Azure AD CBA for more information.

Q: Is an ADFS Implementation required to configure CBA?
A: No, ADFS is not required. The optimal solution leverages the native Azure AD CBA capabilities without the need for a federated server such as ADFS. Leveraging native Azure AD CBA capabilities will provide the most integrated features with Identity Protection and Conditional Access Policies and also reduces an organization's on-premises infrastructure overhead/complexity as well as higher security with one less attack factor in the security surface area.

Q: Does Azure AD CBA support certificates issued by 3rd party Certificate Authorities?
A: Yes. Azure AD CBA supports authentication with certificates issued by any Certificate Authority that a customer organization trusts. Azure AD CBA does not provide any of the certificate issuance, or lifecycle management processes for certificates. Any Certificate Authority chain that issues smart cards that a customer organization trusts can be uploaded to Azure AD to support Azure AD CBA. See: How to configure Azure AD certificate-based authentication?

Q: How often do YubiKeys need to be replaced? Is the licensing costs of the key annual?
A: We work to ensure high quality and long lifetime of our products. YubiKeys are IP 68 rated, crush and water resistant with no batteries or moving parts, and have proven to last more than a decade of daily use**.**

YubiKeys can be purchased with two ways:

- YubiEnterprise Subscription with a lower cost of entry, predictable spend, flexibility, and premium support.
- One-time perpetual license model.

Q: If we deploy YubiKeys to our users, do they stop having passwords as a fallback authentication?
A: Today, passwords are still a valid authentication mechanism with Azure AD even when FIDO2 Passwordless security keys or Certificate-based authentication are enabled with YubiKeys. However, Conditional Access Policies can be enabled to enforce the desired authentication strength (public preview) required by your organization. This will ensure that passwords alone cannot be used to authenticate and that FIDO2 security keys or CBA is mandatory. See: Authentication Strength capability with Conditional access policy. You can also set up Authentication strengths that only a specified MFA method like FIDO2 or CBA be used for enforcing phishing-resistant MFA.

Q: Does the YubiKey support native smart card certificate enrollment with ADCS?
A: Yes, the YubiKey can be used to enroll a smart card certificate with native ADCS capabilities. The ideal experience using ADCS can be improved when using the Yubico Minidriver. See these help pages:
https://support.yubico.com/hc/en-us/articles/360013707820

Q: At my company we started to use YubiKeys, but we encountered the problem of adding the YubiKey in the Microsoft profile as a FIDO2 security key and we were also required to register a phone. Is there any possibility to add a YubiKey without the involvement of the registration of a phone?
A: Yes. This is possible to enroll a YubiKey as a FIDO2 security key without enrolling the Microsoft Authenticator and also without enrolling a phone. It is possible to

immediately enroll a FIDO2 security key in 2 scenarios.
1) If the user signs in with a TAP (Temporary Access Pass)
2) If the user signs in with Azure AD CBA.

Q: What happens if your key gets physically broken or lost?
A: The best practice for FIDO2 Passwordless in Azure AD is that the user has a backup YubiKey enrolled with Azure AD so they can retain access to their account without involving the helpdesk or admins. If the user does not have a backup enrolled then engagement may need to be done with the helpdesk to begin their recovery processes before they can regain access to their account.
TAP or Temporary Access Pass is the recommended recovery mechanism from Microsoft for this use-case.
The best practice when using Azure AD CBA will be dependent on your organization's PKI lifecycle processes.

Q: Is the YubiKey a must for Azure AD CBA?
A: No, YubiKeys are not mandatory. Certificates can be directly provisioned to devices themselves with the help of mobile device management (MDM). Additionally other smart card vendor solutions from other vendors will also support CBA, however these may not today be supported from mobile devices. The Azure AD CBA solution for Android mobile devices only works with YubiKeys as the external key storage.
See:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-certificate-based-authentication
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-certificate-based-authentication-mobile-ios#security-key-providers
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-certificate-based-authentication-mobile-android#security-key-providers

Q: Will the biometric YubiKey be FIPS compliant soon?
A:The YubiKey Bio supports FIDO (FIDO2/U2F) only at this time. Our Federal customers, who generally have the highest demand for FIPS (in addition to companies working with the Federal government or other regulated industries), also generally require PIV. We have no immediate plans to FIPS validate the current product as a result. We are exploring adding other protocols to a biometric product and may consider a FIPS validated version at a later date if customer interest warrants it. Today,

the best option when FIPS is required for compliance reasons, is the YubiKey FIPS Series.

Q: Does the YubiKey support the ability to do offline sign-in into the Windows OS when no internet is available?
A: Yes, the solution with Azure AD and YubiKeys supports offline sign-in to Windows. Offline sign-in is supported when using either FIDO2 Passwordless or Azure AD CBA.

Q: Can username-less authentication be provided with Azure AD CBA?
A: No, username-less authentication is not supported with Azure AD CBA. The username is used for home realm discovery (HRD) as well as to look up the user account in Azure AD.

Q: Can a user register two (or possibly more) YubiKeys to their account in Azure AD
A: Yes, this is possible and this is the recommended best practice. A user should register more than one FIDO2 security key so they maintain access to their accounts if the YubiKey is lost or damaged.

Q: How does the YubiKey communicate with an Android or iOS device - Bluetooth?
A: The YubiKey specifically does not support Bluetooth however the YubiKey does support USB, Lightning and NFC.
Specifically for the Azure AD CBA on iOS solution, the solution does work over NFC or Lightning. See:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-certificate-based-authentication-mobile-ios
Specifically for the Azure AD CBA on Android solution, there is no support today for NFC but Microsoft is working to add this feature. The solution on Android currently works over USB. See:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-certificate-based-authentication-mobile-android

Q: What is the best model to use, Azure AD CBA or Azure AD FIDO2 Passwordless, if you don't require FIPS?
A: Using either FIDO2 passwordless or Azure AD CBA are both valid solutions. If your organization already has established PKI practices and smart card issuance processes

Azure AD CBA may be the preferred approach. If your organization does not already have these processes, it may be best to leverage FIDO2 as the preferred approach. Also note that the two approaches are not mutually exclusive and some customers will leverage both credential types on the same YubiKey. Your organization should review the capabilities of each approach to see if they meet your organization's requirements.

Q: Are all YubiKeys FIPS compliant?
A: No, only the YubiKey 5 FIPs series is FIPS compliant. See: https://www.yubico.com/products/yubikey-fips/

Q: Is it possible to unify the user experience for Android and iOS? It's not good to have a different experience for the help desk or users.
A: Today the experiences are different due to constraints of the operating systems. iOS and Android have different levels of native support for smart cards. Microsoft and Yubico will continue to jointly discuss how the experiences can be more unified.

Q: What is the easiest way to enroll a PIV-certificate to a YubiKey?
A: This depends on what processes and tools are already established at your organization. Many organizations find that a dedicated CMS (Certificate Management Solution) is necessary to manage the whole certificate lifecycle. Other organizations find that the native features of ADCS are sufficient. Here is a place you can get started: https://support.yubico.com/hc/en-us/articles/360013707820

Q: Where can we learn more about YubiEnterprise solutions (features, price)?
A: Here is a good place to start:
https://www.yubico.com/products/yubienterprise-subscription/
You can also find our yes, offerings available on both Azure Marketplace and AWS Marketplace. Contact sales@yubico.com for more details.

Q: Once you authenticate via a key, do you have to keep the YubiKey plugged in?
A: No, the user is not required to keep the YubiKey plugged in.

Q: Is the certificate stored in the mobile device or is the YubiKey required during every auth?

A: The public certificate may get stored on the mobile device. However the private key always remains protected on the YubiKey and cannot be exported.

Q: How are you managing YubiKeys? What are the options for managing the YubiKey lifecycle? Is there any centralized location for managing YubiKeys?
A: Some customers prefer to have a dedicated CMS to manage certificate lifecycles and YubiKey certificate provisioning. Other customers leverage the native capabilities of ADCS for their PKI lifecycle. Some customers also take advantage of YubiEnterprise subscription and rely on the user-based licensing model. A CMS solution is not explicitly required to leverage Azure AD CBA, but customers should review their requirements. When registering FIDO2 security keys with Azure AD, the keys can all be self-service registered and managed from the user's registration portal. See details on how to register FIDO2 security keys.

Q: The Azure AD CBA showed YubiKey as a OTP. Is that correct?
A: No, OTP is not used during the Azure AD CBA with YubiKey solution. The solution uses a smart card certificate to authenticate to Azure AD.

Q: Is this FIPS 140-2 compliant?
A: The YubiKey 5 FIPS details can be found here:
https://www.yubico.com/products/yubikey-fips/

Q: Why is passwordless authentication with the Microsoft Authenticator app less secure than Azure AD CBA or Azure AD FIDO2 Passwordless?
A: One of the requirements for phishing-resistance is that the protections are built into the protocol. CISA guidance is here:
https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
Here are more details about Azure AD Conditional Access policy and the out-of-the-box phishing-resistant authentication strength
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths#built-in-authentication-strengths
Yubico's guidance for phishing-resistance can be found here:
https://www.yubico.com/resources/glossary/phishing-resistant-mfa/

Q: How come FIDO2 with a YubiKey works with iOS and Safari on Mac but not Azure AD authentication?
A: Microsoft is working to enable users to use FIDO2 security keys to authenticate from Safari.

Q: When will MFA custom policy be available in the final release instead of preview?
A:Microsoft is working to release the feature to GA and will announce as soon as possible.

Q: What should I know about derived credentials for FIDO2?
A: When NIST finalizes their guidelines, we expect to have more to share around supporting this new capability.

Q: Will FIDO2 authentication be supported on Android and iOS with NFC?
A: Microsoft has this feature on their roadmap, but no target date is available yet.

Q: Are there advantages to USB C vs USB A? Does Lightning YubiKey work with iPhones and iPads?
A: No, there is no advantage to using USB C over USB A. It is dependent on your device and use cases. Also, many of our YubiKeys are also equipped with NFC which work with iOS with the Azure AD CBA solution.
Yes, the YubiKey 5Ci with Lightning connector does work on iPhones and iPads when using Azure AD CBA.

Q: Can you enroll an ADFS smart card certificate on a YubiKey Bio with the Yubico client?
A: No, the YubiKey Bio series only supports the FIDO protocols. Smart card certificates cannot be enrolled on the YubiKey Bio.

Q: Are there any plans from Yubico to develop a soft token that can be used on users existing devices using Bluetooth Low Energy technology?
A: While Yubico previously initiated development of a BLE security key, and contributed to the BLE U2F standards work, we decided not to launch the product as it does not meet our standards for security, usability and durability. BLE does not provide the security assurance levels of NFC and USB, and requires batteries and pairing that

offer a poor user experience. However, we do offer options that support NFC and USB that do meet our standards. We have no plans for a soft token at this time.