Passwordless. Can it be done?

Joey Cruz @404cruX
Mark Morowczynski @markmorow
Program Managers – Microsoft
Agenda

- The Problem with Passwords
- What is Passwordless?
- Windows Hello for Business
- Authenticator App
- FIDO2
- Go do’s
- Resources
The Most Common Attacks use Passwords

- **Password Spray**
  - 730,000 accounts compromised in last 4 months of 2019

- **Phishing**
  - 60% increase in Phish emails in 2019

- **Breach replay**
  - 5.5 billion accounts with leaked credentials in 2019
Agenda

- The Problem with Passwords
- **What is Passwordless?**
- Windows Hello for Business
- Authenticator App
- FIDO2
- Go Do’s
Can You Go Passwordless Today?
Getting Started With Passwordless

- Doesn’t mean removing all passwords first!
- Use passwords less
- Applications integrated with Azure AD
  - O365, WorkDay, SalesForce, LOB Apps, App Proxy
- Applications that use IWA authentication
  - Internal sites like SharePoint, File Servers
Passwordless Options

High security, convenient methods of strong authentication

Windows Hello for Business

Authenticator App

FIDO2
Agenda

- The Problem with Passwords
- What is Passwordless?
- Windows Hello for Business
- Authenticator App
- FIDO2
- Go Do’s
Windows Hello for Business – Use Cases

- I’ve deployed MFA ...
  - Users - “I get prompted for TOO much MFA!”
  - Incident Response - “they approve all the MFA request they get”
  - Security - “We need more MFA!”

1 user to 1 device
Ex. Information workers
Improve user experience without reducing security
Windows Hello for Business 😊
Requirements

- Azure AD & Azure AD Connect
- Multifactor Authentication
- Windows 10 1709 or later
- Domain/Forest Functional Level 2008 R2+
Hybrid Deployment

Cloud Deployment

On-premises Deployment
Hybrid Deployment

Key Trust (Recommended)
- NO PKI Infrastructure Required (CA role on DCs required)
- Requires Server 2016+ DCs (Some/Not all)

Cert Trust (if you need RDP)
- PKI Infrastructure Required
- Requires client issued certificates
- AD FS Required
Cloud Deployment

Key Trust (Recommended)
- NO PKI Infrastructure Required (CA role on DCs required)
- Requires Server 2016+ DCs (Some/Not all)
Windows Hello for Business

Authentication – Azure AD Joined in Managed environments

User Dismisses locked Screen | Show WHFB CP

User Provides Bio/PIN

Request Nonce

Sign Nonce WHFB privkey

Signed Nonce

Validate WHFB Privkey & Nonce

PRT w/Session Key

Decrypt Session Key w/Transport key

Import Session Key to TPM

Successful Auth

Load User Desktop
Windows Hello for Business 😊

Can it be done?
Athletic Clothing Company

Goals:

• Win10 deployed – 1 user to 1 device
• Needed managers to gain SSO access to applications
• Reduce MFA Prompts
Athletic Clothing Company

Solution:

• Scoped deployment for Win 10 Managed Devices
• Enabled Automatic Enrolment for onboarding
• Windows Hello for Business satisfied MFA challenge
Windows Hello for Business 😊

Can it be done?
YES!
Windows Hello for Business – Do’s & Don’t’s

Do: Deploy Key Trust
Do: Make sure have a Self-Service Password Reset
Do: Plan app modernization LOB apps for Modern Auth

Do Not: Use Convenience PIN (Windows Hello) Disable via Policy
Do Not: Deploy On-premises only – No migration to Hybrid
Do Not: Deploy ADFS unless you absolutely must
Agenda

- The Problem with Passwords
- What is passwordless?
- Windows Hello for Business
- Authenticator App
- FIDO2
- Go Do’s
Authenticator App – Use Cases

• What about my other users macOS/iOS/Android/Linux?
• Field workers - Tablets
• Conference Rooms
• BYOD – Home PC
Password-less Phone Sign-in
Password-less Phone Sign-in

Microsoft Authenticator app to sign in:
- Tap the number you see below in your Microsoft Authenticator app to sign in.

Using the number 83 to sign in:
- Enter the correct number to sign in.

Options:
- Approve sign-in
- Use your password instead
- Deny
Requirements

- Azure AD
- Enable the Combined Registration (MFA & SSPR)
- Microsoft Authenticator App
User goes attempts to AuthN

Browser

User matches number prompted to number on auth app

Auth App

Azure AD

Notifications Systems

Use provides Bio/PIN to unlock Priv Key

Sign nonce with priv key

Key validated and number matched

Generate Session and Sends Push notification

Session issued access token
Authenticator App

Can it be done?
Payroll & HR Service Company

Goals:

- Provide Passwordless for cross platform environment
  - macOS, Windows, iOS, Android
- Avoid SMS Cost for end users
- Wanted to drive users awareness to MFA activity
Payroll & HR Service Company

Solution:

- Enabled SSPR & MFA Converged registration
- Scoped deployment of Passwordless Authenticator App to groups
- End User Communications
Authenticator App

Can it be done? YES!
Authenticator Do’s and Don’ts

Do: Enable Converged SSPR/MFA Registration
Do: Enable end users to report fraud
Do: Establish a process for investigating “MFA Denied by user”
Do: Enable Authenticator for everyone, scope the converged registration (bug)

Do Not: Try to register Passwordless Authenticator App in multiple tenants
Agenda

• The Problem with Passwords
• What is Passwordless?
• Windows Hello for Business
• Authenticator App
• FIDO2
• Go Do’s
What is FIDO2?

- FIDO Alliance
  - Launched in February 2013
  - Develop and promote authentication standards that help reduce the world’s over-reliance on passwords and address security concerns in MFA (unphishable strong auth)

- WebAuthn
  - Extensible web authentication API, part of W3C standards

- CTAP2
  - Extensible client-to-authenticator protocol

- Public/Private Key infrastructure
  - Private keys are securely stored on the device

- Data bound to a single device
- Local gesture (e.g., biometric, PIN) required
Good FIDO2 Use Cases

- 1 user to many devices
- Kiosks (plant worker)
- Unable to bring a phone (retail)
- Admin accounts (also break glass)
Passwordless with FIDO2 security keys

Open standards that allow innovative offerings from partners, serving broad range of user needs

USB/NFC Key  USB Biometric Key  NFC Badge
Requirements

- Windows 10 version 1903 or later
- Azure AD Join device
- Azure Multi-Factor Authentication
- Converged SSPR/MFA Registration
- Compatible FIDO2 security keys
FIDO2 – Security Key

Registration

User

Browser

Registration Panel

Azure AD

User goes to Security info

Insert Key / touch or pin

Verifies RP matches origin
Generates Pub/Priv Key

Verify NGC Claim
Add key process
Nonce RP

Returns if no claim found

Verifies RP matches origin

Returns Pub key, signed nonce, Cred ID

Verifies and registers Pub Key, Stores cred ID
FIDO2 – Security Key

Authentication

User goes to Site or Device

User

User locks device with Bio/Pin

Inserts Key

Signs nonce and request PRT

User unlocks Private key with Bio/Pin

Azure AD issues PRT & TGT

Signs nonce and request PRT

Finds Cred ID and sends Cred ID and nonce

Azure AD

Verifies nonce

Device sends Auth Request

Browser or Device*

Sign in with key

Device Sends Auth Request

*Browser or Device refers to the device the user goes to.
What about on prem resources?
Hybrid Deployment Components

1. Latest version of AAD Connect (1.4.32.0 or later)
2. Latest Windows Insider Build (18945 or later)
3. Patch for Domain Controller (Server 2016 (KB 4534307) /2019 (4534321))
1. User authenticates to Azure AD with a FIDO2 security key.

2. Azure AD checks the tenant for a Kerberos server key matching the user’s on-premises AD Domain.
   - Azure AD Generates a partial Kerberos Ticket Granting Ticket (TGT) for the users on-premises AD Domain. The TGT contains only the user SID. No authorization data (groups) are included in the TGT.

3. The partial TGT is returned to the Windows along with Azure AD Primary Refresh Token (PRT).

4. Windows contacts on-premises AD Domain Controller and trades the partial TGT for a full TGT.

5. Windows now has Azure AD PRT and a full Active Directory TGT.
Can it be done?

FIDO2
Oil & Gas company

Goals:

• Migrate away from ADFS & PKI
• Replace Smart Cards
• Shared Devices
• Users with no Phone
  • No Cell signal
• Need Secure access with SSO to both SaaS & On-prem
Solution:

- Scoped users for FIDO2
- Enrolled Users with MFA and issued FIDO2 Key as part of onboarding
- Established process to for Key Lifecycle
Can it be done?
YES!

FIDO2
FIDO2 – Do’s and Don’t’s

Do: Enable Converged SSPR/MFA Registration
Do: Enroll user in MFA
Do: Scope deployment to those that need it
Do: Plan for key life cycle

Don’t: forget about key logistics (customs)
Don’t: Confuse WebAuthN and CTAP
Agenda

- The Problem with Passwords
- What is Passwordless?
- Windows Hello for Business
- Authenticator App
- FIDO2
- Go Do’s
Go Do’s

Monday
- Define passwordless use cases
- Test FIDO2 for admins
- Understand WHFB prerequisites
- Enable SSPR & MFA
- Deploy Azure AD Password Protection

1 Month
- Start a WHFB & Auth App pilot
- Understand apps to integrate with Azure AD
- Get Executive Buy in
- SSO to Azure AD (Benefits of protection)

3 Month
- Expand WHFB & Auth App pilot
- Start a FIDO2 pilot
- Take advantage of Cloud App
  Discover (Shadow IT)
- Start updating LOB apps to use
  modern auth (MSAL)
Questions

Joey Cruz  
Mark Morowczynski
Program Managers – Microsoft
Resources

• Decision makers: aka.ms/gopaswordless
• Azure AD Deployment Plans: aka.ms/deploymentplans
• How-To Videos: aka.ms/AzureADVideos
• Applications / SDK’s use WebAuthN: aka.ms/passwordlessAPIs
• Azure AD Architecture Videos: aka.ms/identityyoutube