The Windows Hello for Business:
Protocol Level Deep Dive

Obaid Farooqi

Sr. Escalation Engineer

Microsoft

Introduction

- Obaid Farooqi
- Microsoft
- Sr. Escalation Engineer in Developer Support: Protocols Team
- Support Developers implementing Open Specification (https://docs.microsoft.com/en-us/openspecs/)
- Questions on Open Specifications? Send an email to dochelp@microsoft.com

Samba IO Lab

September 16-22, 2019
Microsoft Campus
Redmond, WA

Microsoft

Agenda

- What is Windows Hello for Business (WHFB)?
- Provisioning of WHFB
- Authentication in WHFB
- Q&A

What is Windows Hello for Business (WHFB)?

- A new way of logging in to Windows devices
- Uses Gestures (PIN, Finger Prints, Face Recognition) instead of password
- Uses Asymmetric keys for Authentication
- Gestures are not passwords; they unlock TPM
- Two-factor Authentication. Something you have: Device, something you know: Gesture
- Uses TPM for storing Private key. Even the OS does not know the Private key.
- Domain controllers have knowledge of Public key only. If DC gets compromised, all a hacker gets is public keys

Trust Modes

- WHFB uses Two types of Trust Modes
- Key Trust
  - Uses Key-pair for Authentication
  - Client uses self-signed certificates.
- Certificate Trust
  - Uses Key-pair for Authentication
  - Uses Certificates issued by Enterprise Certification Authority for Authentication (like Smart Card)

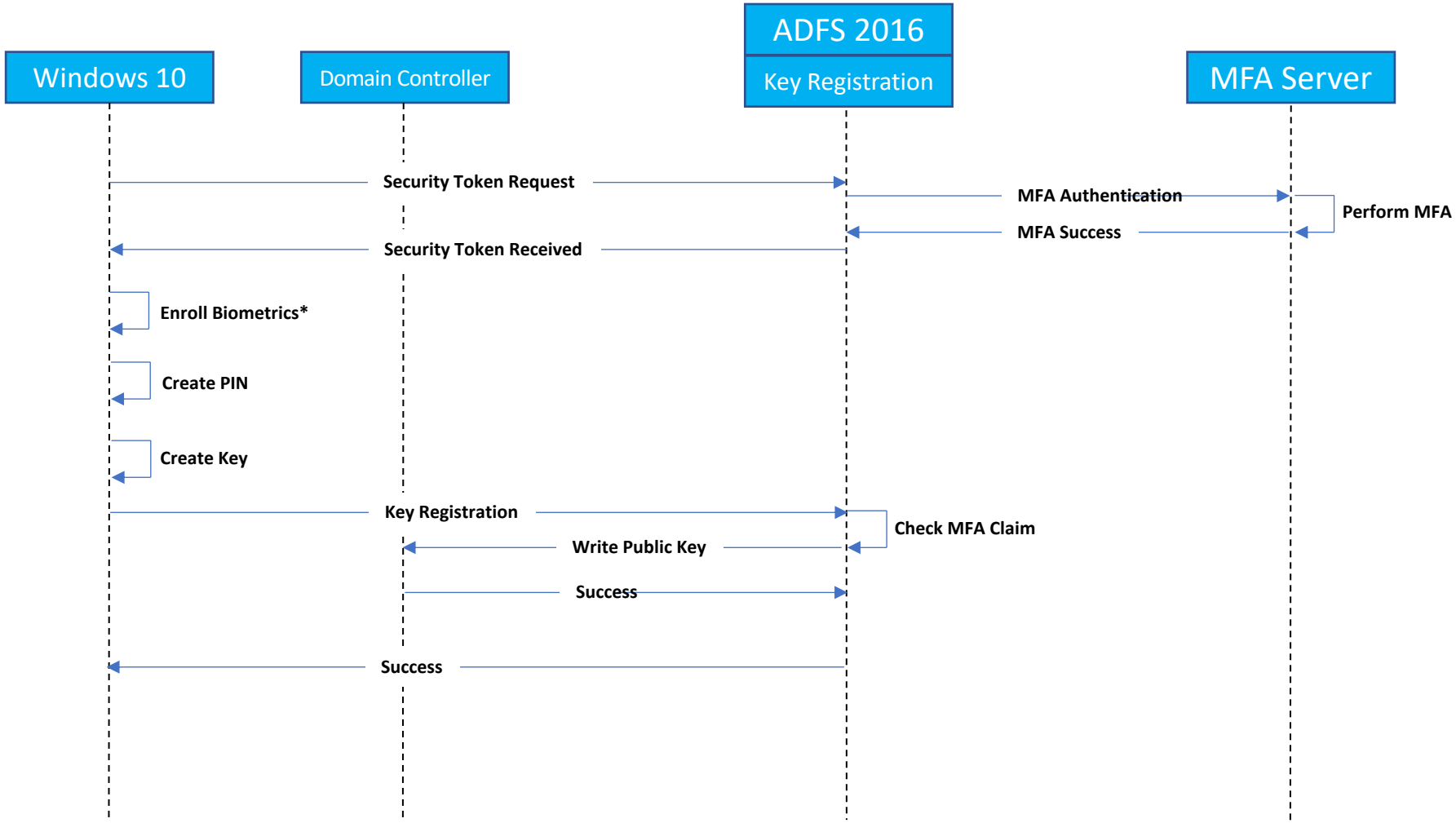
Software Requirements

Key Trust	Certificate Trust
Windows 10, version 1703 or later	Windows 10, version 1703 or later
Windows Server 2016 Schema	Windows Server 2016 Schema
Windows Server 2008 R2 [illegible]ain/Forest functional level	Windows Server 2008 R[illegible]main/Forest functional level
Windows Server 2016 or later Domain Controllers	Windows Server 2008 R2 or later Domain Controllers
Windows Server 2012 or later Certificate Authority	Windows Server 2012 or later Certificate Authority
Windows Server 2016 AD FS with KB4088889 update	Windows Server 2016 AD FS with KB4088889 update
AD FS with Azure MFA Server, or AD FS with 3rd Party MFA Adapter	AD FS with Azure MFA Server, or AD FS with 3rd Party MFA Adapter

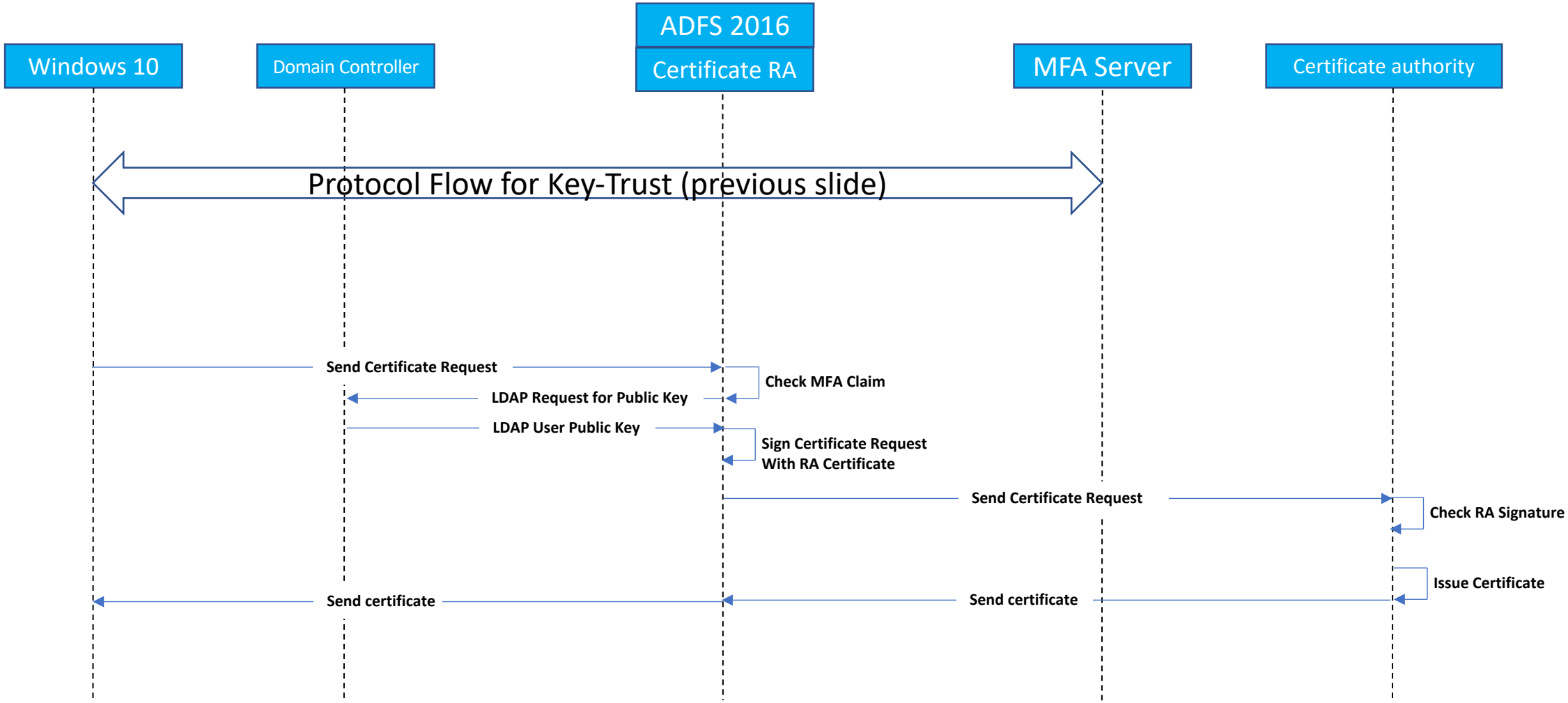
Agenda

- What is Windows Hello for Business (WHFB)?
- Provisioning of WHFB
- Authentication in WHFB
- Q&A

Protocol Flow for Key-Trust Provisioning



Protocol Flow for Certificate-Trust Provisioning



Documents updated for Windows Hello Provisioning

- [MS-KPP]: Key Provisioning Protocol
  - Describes the details of key provisioning Protocol b/w Client and ADFS
- [MS-OAPX]: OAuth 2.0 Protocol Extensions
  - Allows to client to request that MFA be used before a token is issued for key provisioning.
- [MS-OAPXBC]: OAuth 2.0 Protocol Extensions for Broker Clients
  - Allows client to ask ADFS to issue a certificate.
- [MS-OIDCE]: OpenID Connect 1.0 Protocol Extensions
  - Allows server to indicate that it supports exchanging a primary refresh token for a user authentication certificate.

Mapping of Documents to Protocol flow

- Token request for Key Provisioning
  - MS-OAPX
  - MS-OIDCE
- Key Provisioning
  - MS-KPP
- Storing Public Key to AD
  - Lightweight Directory Access Protocol
- Certificate Enrollment from Windows 10 to ADFS
  - MS-OAPXBC

Group Policy Settings for WHFB

- Settings for both **User configuration** and **Computer Configuration** under **Policies>Administrative Templates>Windows Components> Windows Hello for Business**
- Following Settings are required for WHFB
  - Use Windows Hello for Business
  - Use a hardware security device
  - Use biometrics
  - PIN Complexity
  - Use certificate for on-premises authentication (to enable Certificate Trust)
- For details about these settings, please consult the following document

  https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-manage-in-organization

Agenda

- What is Windows Hello for Business (WHFB)?
- Provisioning of WHFB
- Authentication in WHFB
- Q&A

Authentication

- WHFB leverages Kerberos
- WHFB utilizes Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)
- AS-REQ and AS-REP look same as in the SmartCard authentication
- No new fields added to any Kerberos message
- PAC contains NTLM password hash so applications that need NTLM can still function.

Authentication Flow for Key Trust

- User performs gesture (PIN or biometric) to unlock TPM
- Client sends AS-REQ. Preauth data signed with private key in the TPM. Contains a self signed certificate of the client
- WS 2016 DC verifies the signing authority of the certificate and fails
- WS 2016 DC ignores the error and extracts the public key from the self signed certificate.
- WS2016 DC searches in msDS-KeyCredentialLink for matching Private key. Also UPN in AD is verified against UPN in AS-REQ. On success, the rest of the processing happens like the SmartCard Authentication

Authentication Flow for Certificate Trust

- User perform gesture (PIN or biometric) to unlock TPM
- Client sends AS-REQ. Preauth data signed with private key in the TPM. Contains the user certificate issued by Enterprise Certificate Authority (CA)
- AS-REQ is sent to Windows Server 2016 DC (KDC)
- The rest of the processing is like the SmartCard Authentication

Documents updated for Authentication

- [MS-PKCA]: Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol
  - For Certificate-Trust:
    - The protocol flow is same as Smart Card Authentication
  - For Key-Trust:
    - A section for Key-Trust is added in MS-PKCA (3.1.5.2.1.4 Key Trust)
    - User sends Public Key in the AS-REQ in a self-signed certificate
    - Server (WS2016 or later) ignores failure of certification chain verification and extracts the Public key from certificate
    - If the Public key matches with one of the keys in User object (msDS-KeyCredentialLink attribute), the server continues the processing

Certificate Expiration

- Applies to Certificate Trust only
- Certificate is automatically renewed before it expires
- The following Group Policy setting is configured for automatic renewal:
  - **Certificate Services Client – Auto-Enrollment** under **User Configuration>Policies>Windows Settings >Security Settings>Public Key Policies**
  - Details at https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings
- Password expiration has no effect on user authentication certificate and vice versa

Refences

- Windows Hello for Business Reference

  https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification

Thank You!

Questions?