Standard Operating Procedure – Configure Azure Entra for FIDO2 Authentication and Register User FIDO2 Passkey

1.0 Purpose:

The purpose of this SOP is to document the configuration of the Thales Azure Entra identity provider to accept and register FIDO2 security authentication tokens.

1.1 Server/Machine affected:

- Azure Entra portal

1.2 Materials Required:

- Credential with at least Authentication Policy Administrative access role to Azure Entra
- Thales E-token Fusion FIPS security token (tested keys with both FIDO 2.0 and 2.1 applet)

1.3 Prerequisites:

- Workstation with access to azure portal.
- Note: Microsoft Edge browser seems to be more stable than Chrome when working with FIDO2 registration on the Azure portal.

2.0 SOP Tasks:

Step 1. Sign in to the Azure Portal and navigate to the Entra Admin center. Please note that this is different than the traditional Azure AD Identity interface.

1) Open a browser and navigate to Portal.Azure.US. (Tested with gov/national Azure cloud)
2) Enter username and password credentials.
3) Navigate to the Microsoft Entra ID admin console.

Step 2. Enable passkey authentication

1) Navigate to the Entra portal (Entra.Microsoft.US).
2) In the left menu bar, expand protection and select “Authentication Methods”.
3) Under Authentication methods select manage “Policies”.
4) Left click on FIDO2 Security key.
5) Click the “Enable” option and select save.

Step 3. Add a step-up authenticator

1) Navigate to myaccount.azure.us.
2) Login as the user that needs to register a new security key. The Entra identity password will be required.
3) In the left menu, click on security info.
4) At the security info page, left click “Add sign-in method”.
5) Select phone from the drop down list.
6) Select add.
7) Enter the phone number of the mobile phone that will be sent the TOTP code.
8) Select next.
9) Enter the received code and select next.
10) At the verification complete screen, select done.

3.0 Step 3. Register a security key for a user

1) Navigate to https://myaccount.azure.us.
2) Login as the user that needs to register a new security key.
3) In the left menu, click on security info.
4) At the security info page, left click “Add sign-in method”.
5) At the “Add a method” window, expand the drop down and select security key.
6) Left click add.
7) The registering user will be prompted to sign in using two factor authentication. Select next.
8) Select next to step up authenticate using TOTP.
9) At the “Verify your identity” prompt select the defined phone number for TOTP.
10) At the “Enter code” prompt, enter the received code.
11) Left click verify.
12) At the “Security key” prompt, select USB Device.
13) At the “Security key” prompt, select Next.
14) At the “Create a passkey on a phone or tablet” prompt, select “Save another way”.
15) Select external security key.
16) At the “Security Key Setup” prompt, left click OK.
17) Select OK to continue setup.
18) Enter the security key PIN, twice.
19) Left click OK.
20) Touch the security key to prove presence.
21) Enter a name for the Security Key.
22) Left click Next.
23) At the “Security Key” prompt, left click done.

Step 4. Access Azure resource using FIDO2 key. (Azure portal for this example)

1) Navigate to portal.azure.us.
2) Enter the full user identity name. (e.g. FIDO2Test@ThalesTCT.onmicrosoft.us.)
3) At the “enter password” prompt, select “Use your face, fingerprint, PIN or security key instead”
4) At the “Use a saved passkey for login.microsoftonline.us”, select “Windows Hello or external security key”.
5) Enter the security key PIN and left click OK.
6) Touch the security key contact point to complete FIDO login.