ensurity
A Step Ahead!

Use Case - Banking

# Implementation of **FIDO2 Authentication** for Core Banking and Azure joined Applications

**CUSTOMER** : A leading Bank in Abu Dhabi

**DATE OF IMPLEMENTATION** : March 2023

**ENVIRONMENT** : Hybrid AD along with several Local AD's, Firewalls.

**PROBLEM STATEMENT** :

a. Eliminate vulnerabilities with single factor authentication and prevent password sharing

b. Discard Soft authenticators with attributable keys

c. Central Key Management across various geographic locations.

d. Tailored key functionalities:

- PIN Control
- Enrolling fingerprints in a secure environment
- Limit key reset and restrict new self-enrollments
- Reassignment, reactivation, locking, and other functions are all centralized.
- Locked to Bank Azure AD account.

## Solution Offered

Ensurity has provided its Biometric FIDO2 security keys with its Life Cycle Management software (Asset Management System) to fulfill the specified requirements of the bank.

a ThinC-AUTH Biometric Security keys

b Life Cycle Management Software Solution

c Ensurity customized the Security Keys

### a ThinC-AUTH Biometric Security keys

Ensurity Integrated its ThinC-AUTH Biometric FIDO2 keys with the bank's Hybrid AD environment providing Single sign on to all applications including Core Banking. The solution enables users to access their applications by utilizing centrally managed Biometric security keys for login, eliminating the need for conventional passwords. This approach mitigates the risks associated with phishing and unauthorized sharing of credentials.

## b Life Cycle Management Software Solution

To streamline the centralized deployment & management of hardware keys across locations, Ensurity implemented its **Asset Management System (AMS) i**n the bank's data centre, with no external access. AMS provides the following functionalities:

a. Easy Inventory Management of ThinC-AUTH Biometric Security Keys

b. Identity integration — User syncing with Bank's AzureAD

c. Login to the AMS portal with AzureAD assigned MFA

d. Assign Roles to the Users (Admin / Service Desk / Generic User)

- 'Admin User' can import the device list into the AMS and assign the Keys with Users
- 'Service Desk User' can send invites to the selective User(s) to enroll their fingerprints onto their Biometric Security Keys
- 'Generic User' can only enroll his/her fingerprints onto the assigned Biometric Security Key

e. Easy assign/unassign Keys to Users

f. Automated eMails to the User regarding the Security Key assignment status

g. Controlled environment for enrolling user fingerprints onto the Biometric Security Key (only through AMS Agent Tool)

h. Provision to set a choice of maximum fingerprints (between 1 and 5)

i. Mandate the authentication with Biometrics (dynamic generation of random PIN, which is unknown to the User)

j. Reset the ThinC-AUTH remotely for removing the Fingerprint Data of previous User (only through AMS Agent Tool)

k. Log Management

- Device Log (fingerprint enrolment status on the Security Key)
- Event & Audit Logs (login & activity details)
- Export Logs as Excel files

## c Ensurity customized the Security Keys for the following functionalities:

a. FIDO2 authentication for WebAuthn-enabled applications and compatible Windows 10 (Ver 1903) and above releases

b. Dynamically generated PIN for every Key – for enrollment

c. Disable PIN fall back to avoid willful misuse of the key

d. Locked to single Microsoft account (user cannot add a second account)

e. User cannot reset the Security Key within the Windows tool

f. Configurable count for enrolling maximum fingerprint

g. Remote 'ReVset' through Ensurity's AMS (Asset Management System) portal

**Thus, Ensurity has fulfilled the banks requirement with a complete life cycle solution with its AMS and customized FIDO2 Biometric Security Key. Using the solution, Bank users could securely access their applications using FIDO2 Biometric Security Key.**