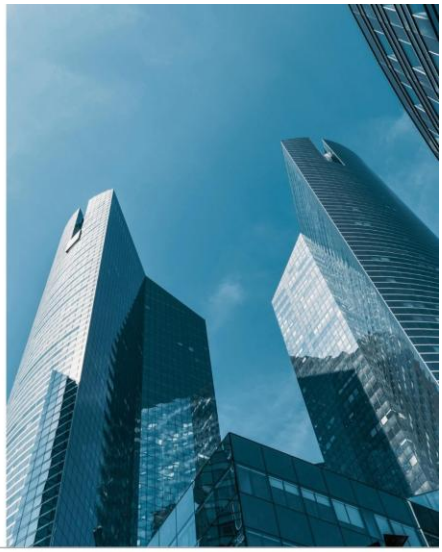
InnaIT IDENTITY SECURED | PRECISION BIOMETRIC

CASE STUDY

FLEXCUBE INTEGRATION

INDUSTRY - BANKING, FINANCIAL SERVICES AND INSURANCE



www.innait.com

This integration was done for an Indian private sector bank headquartered in Thrissur, Kerala. The bank has 245 branches and 258 ATMs/CDMs spread over the states of Kerala, Tamil Nadu, Karnataka, Andhra Pradesh, Telangana, Maharashtra, Gujarat, Delhi, West Bengal, Madhya Pradesh, Punjab, Uttar Pradesh, Rajasthan, Chandigarh, and Haryana.

OBJECTIVE OF THE BANK

To enhance security by implementing Two factor authentication using biometrics for their Critical Applications (CBS and other applications)

THE EXISTING SYSTEM USED BY THE BANK

- No. of users: 2,000+ concurrent users
- CBS – Flexcube
- The critical applications were protected by Single Factor Authentication (Password)
- Problems with the conventional 'User ID & Password' based security systems:
    - Password/Identity theft was possible and exchange of password amongst colleagues in emergency situations
    - Periodic password changes required to ensure data security
    - External hacking of the system was possible

THE BANK'S REQUIREMENT

- Regulatory compliance
- Biometric comparison should be < 40 milliseconds for each transaction & < 1000 milliseconds for the entire transaction
- Fingerprint template should be encrypted to a single unbreakable string
- Raw image provided to client side and given a randomly generated encrypted file name and stored in database

HOW PRECISION HELPED SOLVE THE ISSUE

Precision Biometric proposed InnaIT Framework. Applications to be integrated with solution and provide the required Biometric based two factor authentications for Application login.

InnaIT – 2FA: The solution is designed to integrate the Biometric solution in a client server / browser-based environment. 2FA solution consists of the below mentioned four components:

Client Driver – The client-side driver contains the fingerprint capturing and extraction process. This is installed in every client system

Server Component – The Server Component contains the fingerprint comparison components in Microsoft .NET Environments, Java etc

Software – InnaIT – 2FA

Hardware – Scanner will be connected to every PC/ Thin client via USB port

Enrolment is done through the scanner (at the client), where the individual fingerprints are scanned. The captured data is stored as digital templates (minutiae) in the Central server. During the comparison or verification process the user is identified using fingerprint that is compared to the user's previously registered fingerprint on the server. If the fingerprints match, the user is "verified". As the live fingerprint is compared to only one stored fingerprint, this is called a one-to-one matching process (1:1). As in the enrolment process, when fingerprint verification is done, only the fingerprint template is used in the comparison, not the actual image of the fingerprint.

HOW DID IT BENEFIT THE BANK?

This integration by Precision helped the bank tie Logins and individual transactions to actual people (Audit Trail), this also makes complex password policies easy. The implementation preserves confidentiality of sensitive data & ensures conformity to laws, regulations, and standards