



CASE STUDY

Innait IMPLEMENTATION

IN ONE OF THE LARGEST PRIVATE SMALL FINANCE BANK

INDUSTRY - BANKING, FINANCIAL SERVICES AND INSURANCE



www.innait.com

One of India's largest Small-Finance Banks & a Fortune India 500 Company.

PROBLEM:

The Bank uses Oracle's Flexcube as its Core Banking Solution (CBS). The employees were using a traditional username and password methodology along with OTP to log in to the CBS. Considering the risk factors of Credential compromise and the recurring cost of OTP incurred thereof, The Bank decided to implement the '**Identity First Digital Trust**' approach by implementing a Multi-Factor Authentication (MFA) methodology using Biometrics in compliance with the Reserve Bank of India's (RBI) Guidelines.

HOW PRECISION HELPED SOLVE THE ISSUE?

Precision proposed a secure SaaS model-based **Workforce Identity & Access Management (WIAM)** solution that included the Innait server stack, Software Token Mobile App (Soft-Token App) and Integration to the Bank's CBS application. The solution completely eliminates the use of SMS-based OTPs and replaces it with frictionless and Best-in-Class security combining Native Biometrics and PKI. The Innait server stack is also **CERT-IN certified** (CERT-IN is a Nodal Cybersecurity agency of India, under the aegis of the Ministry of Electronics & Information Technology, MEITY).

The Soft-Token App generates a unique **Key-pair** (Public & Private Key) during user registration, storing the public key on the Innait server and the private key in an encrypted form inside the user's mobile phone (The private key never leaves the phone). This private key is used to identify the user (Digital certificate) during authentication and provide access.

At the time of login, the user visits the InnaIT URL, which triggers a fingerprint verification request on the Soft-Token App on the user's phone. Upon successful fingerprint verification, a list of authorised applications based on the user's role will be shown. The user chooses the CBS application from this list. The user is then redirected to the CBS login page, where they need to enter only the CBS password and gain access to the CBS application. The soft token also captures the user's **geo-location** (basis GPS) when the authentication is initiated, thus identifying the location from where the user is logging in. Precision is also working with the Bank to enable **Geo-Fencing** of users as an additional feature so that they can ensure that the user is within the bank premises when logging into their applications.

IMPLEMENTATION:

In the first phase, the InnaIT Workforce Identity & Access Management (WIAM) solution has been implemented for 10,000 CBS users. In the subsequent phases, this would be expanded to the entire workforce of 35,000 users for CBS, HRMS and other applications, enabling Single-Sign-On (eSSO) solution for their users.

HOW DID IT BENEFIT THE ESTABLISHMENT

- Best-in-class Information security with Biometric (What you Are) and PKI-based authentication for MFA.
- The 'Role-based application Access' to restrict the user to access only authorised applications.
- Friction-less OTP-less access enhances the productivity and reduces cost.
- Geo-location capture creates a non-repudiable log of the user's location during the authentication.
- There is no centralised storage of Biometric data, enhancing security further.
- User Access Logs are captured for Audit & Compliance.
- The integration is easy as the InnaIT solution supports OpenID and FIDO Standards, enabling quick implementation.