



## CASE STUDY

# InnaIT INTEGRATION - SAP

BIOMETRIC AUTHENTICATION FOR A LEADING ELECTRONICS AND  
DEFENSE SYSTEMS MANUFACTURING ORGANIZATION

INDUSTRY - ELECTRONICS AND DEFENSE SYSTEMS MANUFACTURER

[www.innait.com](http://www.innait.com)

## Introduction

In today's digital world, where most transactions take place online, maintaining secure services is extremely important. This case study explains how the organisation leveraged InnaIT Integration with SAP to enhance transaction security.

## Background

A premier Indian Government-owned aerospace and defence electronics company operating under the Ministry of Defence designs, develops, and manufactures advanced electronic equipment and systems for the Indian Armed Forces.

## Objective

The primary objective of the organisation was to strengthen security during financial transactions and enable employees to securely access payroll and profile details using InnaIT integrated with the SAP application. This initiative aimed to reduce the risks associated with single-factor authentication methods, such as passwords, which are vulnerable to breaches and unauthorised access.

Within the organisation, SAP serves as a centralised application used across various sectors.

The Finance department uses SAP to process vendor billing, while the HR department uses it to manage employee payroll and profile information. Only authorised personnel are permitted to perform these activities.

To further enhance security, the customer planned to implement biometric-based authentication for approving billing and payroll-related activities within the Finance and HR departments.

Accordingly, Precision Biometric developed a function module in SAP and implemented biometric-based authentication.

## Existing System and Requirement

Before the InnaIT Integration, the customer relied on Single-Factor Authentication (SFA), primarily through passwords. Recognising the limitations of this system, the customer defined the following requirements for the new security solution:

**Biometric Performance:** Fast and accurate fingerprint verification for each transaction and for accessing user privileges.

**Data Security:** Ensuring that fingerprint data is encrypted to prevent unauthorised access.

## Solution Deployed

After careful evaluation, Precision Biometric proposed implementing the InnaIT Framework within the customer's premises to secure transactions in the SAP application. The InnaIT Framework solution consists of four main components:

**Client Driver:** Installed on each client system to generate authentication pop-ups and process fingerprint verification.

**Server Component:** A functional module created within the SAP environment for the HR and Finance sectors.

**Software:** InnaIT ActiveX software enabled seamless integration and smooth fingerprint authentication during transactions. (ActiveX is a technology used by SAP software to enable the integration and embedding of SAP functions and data into other applications or custom solutions.)

**Hardware:** Fingerprint scanners connected to every PC and thin client through USB ports for biometric enrolment and verification.

## Benefits

The implementation of the InnaIT Framework for transaction security delivered several benefits:

**Enhanced Security:** Biometric authentication significantly reduced the risk of unauthorised access and data breaches.

**Improved Audit Trail:** Detailed logs of authentication activities enabled effective monitoring and compliance checks.

**Future-Ready Architecture:** The scalable and flexible solution allowed SAP functionalities to better address evolving security threats.

## Conclusion

The implementation of the InnaIT Framework within the organisation marked a significant step towards enhanced cybersecurity. By adopting this biometric authentication solution, the customer was able to protect sensitive data and strengthen its defence against cyber threats.

This case study demonstrates that, with proper planning and the right technology, large organisations can achieve a high level of security while building greater trust in the digital era.