



CASE STUDY

TWO FACTOR AUTHENTICATION IMPLEMENTATION

INDUSTRY - PHARMACEUTICAL COMPANY



www.innait.com

Background

An Indian multinational pharmaceutical company, which was established in late 60's with >

20 branches all over the world, with a team of over 15,000 employees. A pioneer in introducing latest technology in pharma, it is one of the largest generic pharmaceutical companies by revenue globally. The company's key focus areas include pediatrics, cardiovascular, anti-infectives, diabetology, asthma and anti-tuberculosis.

Objective

To enhance security by implementing Two factor authentication using biometrics for their critical applications

Existing System

- The critical applications were protected by Single Factor Authentication (Password)
- Problems with the conventional 'UserID & Password' based security systems are:
 - Password/Identity theft was possible and exchange of password within colleagues in emergency situations
 - Periodic password changes to ensure data security
 - External hacking of the system was possible

Requirement

- Regulatory compliance
- Biometric comparison should be <40milliseconds 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
- API should be robust to service multiple instances and flavours of the applications

Solution Deployed:

- Precision Biometric proposed InnalT Framework Applications to be integrated with solutions & to provide the required Biometric based two factor authentications for application login
- **InnalT 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 and this is installed in every client system
 - **Server Component**-The Server Component contains the fingerprint comparison components in Microsoft.NET Environments, Java etc.
 - **Software**-InnalT-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". Since 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.

Benefits

- Tie Logins and individual transaction to actual people (Audit Trail)
- Make seven complex password policies easy
- Preserves confidentiality of sensitive data
- Ensure conformity to laws, regulations, and standards