



CASE STUDY

Citrix INTEGRATION

INDUSTRY - BANKING, FINANCIAL SERVICES AND INSURANCE



www.innait.com

BACKGROUND:

The insurance company has its own BPO & customer support center where they provide solutions to customer queries & problems. They use Dell Thin clients with Citrix shared & dedicated VDI, inside the VDI environment. They use many applications integrated with a single SSO system – Key Cloak which uses password as main authentication method.

EXISTING SYSTEM:

Customer was using a module provided by ZOHO which enables Google Authentication with email code verification, which would pop-up when a user attempted to log in. This agent was installed in Citrix environment. Customer experience problems while using this solution since mobile phone is needed to obtain the Google Verification.

Requirements

In line with policies, the client desired to integrate another factor for login options, for both Citrix login (Windows) and Key Cloak. Since this Call Centre is a 'no-mobile' zone, QR or OTP were infeasible as another factor. So, they requested Precision to provide a solution for application and Windows login with biometric technology for authentication.

Solution Proposed

- **Windows Login:** We have introduced InnaltKey to the client. InnaltKey is a PKI enabled biometric device with Win-Logon module-Windows OS Login with two-factor authentication with AD credentials and Biometric based authentication is achieved by using Precision's Credential Provider software loaded on Citrix

Server. At the time of login, user will be providing their AD credentials in the Citrix login page and the same will get validated against AD. On successful AD authentication, Citrix will login & Biometric Fingerprint authentication is triggered & the user needs to scan his/her fingerprint to continue the authentication process. On successful FP authentication user will be allowed to login to their respective Citrix environments. The same validation will happen when the user logs off or locks the Citrix Session.

- **Key Cloak:** It supports open ID & WebAuthn Authentication (FIDO). Since our solution supports both, we have integrated the same with the client's system.

Benefits

- Enhances security with biometric authentication
- Preserves confidentiality of sensitive data
- User access logs for audit & compliance