

## Case Study

**Leading Kuwaiti National Insurance Company Implements Single Sign-On Identity And Access Management Solutions For Risk Elimination, Ease Of Access & Enhanced Productivity.**

☑ Risk Elimination

☑ Ease Of Access

☑ Enhanced Productivity

A leading Insurance Company in Kuwait is a comprehensive insurance provider with a large national customer base & is 100% owned & promoted by Kuwaiti nationals. With one of the most experienced management teams in the GCC (Gulf Cooperation Council), this highly ranked insurance provider is led by a stalwart within the national business community. Its Board of Directors hosts some of the most eminent names in the business ecosphere and the company employs a large permanent workforce. They have consistently rated as market leaders in this particular portfolio for over a decade and provide a wide range of specialized insurance offerings. The company has been a regular user of the 3i-infotech PREMIA product for their General Insurance & Medical Business verticals since several years and reached out for a new requirement for enhanced ROI.

## Technologies Employed

Oracle Database - 11g Release 2

Oracle Fusion Middleware Forms & Reports - 11g Release 2

Oracle Internet Directory - 11.1.1.7 & Directory Integration Platform

Oracle Access Manager -11.1.1.7

Microsoft Active Directory Server - Win 2012

Java J2EE for ORACLE Weblogic, OAM ,OID & Forms & Reports

External Java Authentication for password validation between LDAP directories

---

## The Problem

Streamlining processes and access through multiple Oracle applications with multiple passwords was increasingly difficult & increased security risks. The client sought to authorize all of their in-house applications with a single sign-on solution with their Domain LDAP server, which, in this case, was the Microsoft LDAP. The need was to simplify authorization access against the domain user identification and password, with no further login pages popping up at the application level.

Resource costs were increased due to administrative overheads associated with relatively frequent access privilege updates, lost passwords, registering of new hires and multiple account lock-downs & reactivations. Security concerns were also cited and was a major challenge considering the sensitivity of policy & customer data in the sector. The client requested for Oracle Fusion Middleware 11g Release 2 Forms & Reports with Single Sign-on solution with Microsoft Active directory server.

---

**The client sought to authorize all of their in-house applications with a single sign-on solution. <<**

---

---

## The Solution

---

**3i Infotech identified an Oracle Identity & Access Management Suite solution. <<**

---

Expertise in project recon enabled comprehension of the customer requirement at a holistic level and allowed 3i Infotech to identify an Oracle Identity & Access Management Suite solution specific to the customer's problem. Implementation of the solution required an upgrade to 11g Forms & Premia modules for General

Insurance & Medical Insurance from the existing 10g application. 3i Infotech's proven approach to customization helped design the most suitable solution by integration of multiple Oracle components and finally integrating it into the Microsoft domain server acting as their domain LDAP, the Active Directory server.

---

## Implementation Challenges

---

Microsoft uses a proprietary hashing algorithm called Unicode password encryption that is not supported in OID. OID and OAM support, more commonly used password encryptions such as MD5, MD4, SHA, SSHA and Crypt, whereas Microsoft supports none of these.

The differences in password hashing mechanism chosen between them caused password synchronization issues between Microsoft ADS and Oracle access Manager & OID. Developing the solution required a third party Java plug-in program enablement to act as the external authentication plug-in between Microsoft ADS to OID and OAM, to subsequently pass the credentials to the application side and allowing authorization of the user for login.

## Major Benefits of SSO Solution for Customers



### Lowered Cost of Password Administration

Authorization is taken care of at multiple levels and password reset issues are streamlined.



### Increased Security

Single Sign-on configures automatic log out policies for users to prevent unauthorized access.



### Improved Compliance & Security Capabilities

Specialized SSO creates a simplified procedure for employees, helping them adhere to security policies easily.



### Reduced Fraud

Phishing, a fraudulent process where victims are tricked into giving away sensitive user information, is a threat to more fragile systems. Implementation of SSO creates a robust system structure for users.



### Simplified User Experience

More seamlessness across multiple domains enables a smoother user experience. This is attained by user-logs at a single access point.



### Accelerated User Web Access

When traditional time-consuming user login processes are replaced by SSO, a domain-specific user credential allow login to multiple applications on the same domain.



### Facilitation of B2B Product Collaboration

For large scale product collaborations to work, the participating businesses should be very interoperable. SSO helps with connecting different systems and enables fluid yet secure inter-system data exchange. Since products built on platforms of partner companies is the norm, using SSO helps facilitate communication and easy workflow.

## About 3i Infotech

3i Infotech provides a comprehensive set of IP based software solutions & a wide range of IT services, and has successfully streamlined business operations of customers globally. The company has a global family of 4,500 employees in 20 offices spread across 11 countries, and over a 1,000 customers in more than 50 countries across 4 continents.

Committed to Empowering Business Transformation, the company provides data -derived insightful and customized solutions to its customers across the globe.