Identity Management Deployment

A Healthcare case study

Background: DIT was approached by a large healthcare organization with the intention of seeking assistance in supporting their set of systems and processes that provide healthcare providers trusted and secure access to government e-Health applications. The system consists of a robust identity validation process that uses a person's real-world identity to create a digital identity, as well as an authentication process.

Goals:
The goals of the system include the identification of clients and providers, the assurance of personal health information privacy which will support the creation of a government EHR.

This system provides three main services to health care providers:

- Registration: process that initiates an individual's electronic identity and provides electronic credentials for the individual allowing them access health care applications.
- Authentication: validates the registered identity when the user attempts to access a health care application.
- Authorization: identifies the services a user is allowed to access. An individual receives authorization to access a health care application though an enrolment process involving sponsorship by the custodians of the health care application or their delegates.

Approach: DIT leveraged the following Oracle v11gR2 products to support the three services above as well as the Identify Provider functions:

- Oracle Identity Manager (OIM)
- Oracle Adaptive Access Manager (OAAM)
- Oracle Access Manager (OAM)
- Oracle Identity Federation (OIF)

Major Outcome:
OAAM was successfully installed in front of the client portal prior to our involvement and information on user access to the portal had been logged since then. OAAM was installed in front of additional services at a later time. This login data was intended to provide information that could be used to fine tune the business rules to ensure that the challenge options were defined appropriately.

DIT evaluated the environment, captured data from OAAM, and provided recommendations on the most effective way to leverage Risk Based Authentication as a component of the overall service offering.

Highlights:
There were occasional changes in direction, which required slight scope and schedule revisions. However, the overall changes did not affect the budget, which remained unchanged. The combined team of client staff and DIT staff worked together to create an open project team that was able to communicate and escalate problems for a quick and effective resolution. The client exhibited extraordinary support from its management to make the project a success.