GFIPM Phase III – Lessons Learned

1 Overview

1.1 Executive Summary

To date CTS has completed the R&D on phase III of the project and has installed and configured the necessary Oracle products to complete a proof-of-concept federation. The goal of this document is to describe the lessons we have learned in the R&D, architecting and initial installation and configuration process.

1.2 Project Overview

In May 2009, The Superior Court of California, Orange County (SCOC) was commissioned by the Global Security Working Group (GSWG) and National Center of State Courts (NCSC) to begin research with the goal of developing a series of working production model federations in keeping with the Global Federated Identity & Privilege Management (GFIPM) security model. SCOC's Court Technology Services (CTS) began researching the GFIPM security model in June of 2009 and made the decision to Use Oracle Internet Directory (OID), Oracle Identity Federation (OIF) and Oracle's WebLogic Server (WLS) for security management.

The agreement between GSAC, NCSC and SCOC was to implement the following phases for the project:

- Phase I - Private Defense Attorney Interface (PDAI)
- Phase II - Probation eFiling of Probation Violations using OASIS Court e-Filing Specification
- Phase III - Administrative Office of the Courts (AOC) System Analysis and Program Development (SAP) Interface

This document refers to lessons learned in the R&D on the test implementation of Phase III of the project.

For this phase of the project, our goal was to use Oracle Identify Federation to create an Identity Provider (IdP) that allows a Court user to access The AOC's Courts Protective Order Registry (CCPOR) application using SAML 2.0 Web Browser Single-Signon (SSO) Profile (The AOC is acting as SP for this phase).

2 Lessons Learned

To complete GFIPM Phase III, our development team on the Court side hosting the SAML 2.0 IdP used the following Oracle products: OID (Oracle Internet Directory) 10g, OIF (Oracle Identity Federation) 11g, and WebLogic 11g. OID 10g was used to store our user Identities. OIF 11g was used for the sole purpose of providing a SAML 2.0 IdP. WebLogic 11g was used as the application server to run OIF 11g as a managed server. On the AOC side, WebLogic 11g was configured to serve as an SP (Service Provider) running the CCPOR application.

Our original intention was to use OID 11g for our user identities. However, we were unable to install the product on our server. The installation would always fail at the 95% point. We had to rebuild the entire machine to ensure all the Oracle files were completely removed. This took about 3 hours for each attempt to install OID 11g. We read through Oracle's approximate 500 page document looking for something we missed but it appeared that we were doing everything right. After a few weeks of trial and error with no progress, we filed a SR (Service Request) with Oracle requesting assistance. Oracle support asked for many details of our environment and settings. We kept updating the SR with the requested information but getting nothing useful in return for solving the problem. Ultimately, we realized that the issue was not going to be resolved so we decided to use OID 10g. We installed OID 10g with no problems . Actually, it took about 45 minutes to install OID 10g. The major difference between OID 10g and OID 11g was that OID 10g was bundled with an Oracle database. OID 11g required the installation of specific Oracle database versions and the OID schema objects needed to be installed using a special tool called RCU (Repository Creation Utility). In addition to these dependencies, OID 11g runs as a managed server on WebLogic. Once we had OID 10g installed, we installed an Oracle product called ODS (Oracle Directory Services). This is an Oracle Fusion Middleware component that allows someone administrating identities to get access to OID from a central Administration console. OIF can be accessed from the same Oracle Fusion Middleware console. We found this to be a great feature for supporting multiple Oracle products. Unfortunately, we were unable to use ODS due to memory constraints. OIF 11g takes about 4 GB's of memory, and our server only had 4 GB's of memory. When we started up ODS, the server was operating at 6 GB's of memory and moving in slow motion. Therefore, we had to keep the ODS WebLogic managed server shutdown at all times. As a last note, just recently we tried to install the current version of OID 11g and the install was successful. We can only assume that bug fixes were introduced in the current version.

User accounts needed to be created in OID for the IdP. We used a feature of OID called the Identity Management Self Service Console. It provided an easy user interface for creating new users. Also, Groups can be created for categorizing users.

Another tool for managing users is called OID's Delegated Administration Services (DAS) which provides a set of utilities for management of OID information. Our team found the tool to be very useful to view user details and to manage expiration policies. However, it was not straight forward for creating users because they had to be subclassed from the InetOrgPerson class.

The OIF 11g installation was successful on the first attempt. The real challenge came in configuring the IdP. Since our team was new to the concept of IdP and SP, we were having a difficult time determining where in OIF to configure the IdP and SP. There was an IdP and SP configuration screen. In addition, there was an IdP and SP import Metadata screen for Trusted Partners. Once the Metadata was imported, it needed to be configured. We were initially configuring the OIF IdP to send back the X509 Subject Name. After testing the IdP with WebLogic's built-in SP tester, we realized that our configurations were not taking affect. To our surprise, we needed to configure this in the imported SP Metadata. Once we made this configuration change, the X509 Subject Name was sending. Once we established our IdP, our Superior Court development team worked with the AOC in setting up WebLogic as an SP.

The goal was to pass GFIPM attributes from our OIF IdP to the AOC'S SP. An initial road block was that OIF did not allow ":" colons to be used for an attribute name. GFIPM attributes are made up of multiple colons (i.e. gfipm:2.0:user:GivenName). Since we could not add the attributes in the Front-End of OIF,

we found the underlying XML file that contained the attribute settings. Once we changed these values directly in the XML, the attributes were being sent back from the IdP. The next challenge was to get the WebLogic SP to receive attributes and make a policy decision on them. Unfortunately, there is no support for attributes except for one hard-code attribute called “Groups.” This one attribute can be used to create a role based policy. We did not use this attribute because it is not GFIPM compliant. The approach we took was to use the X509 Subject Name. An example of the X509 Subject Name would be “cn=jsmith,cn=users,dc=ocsuperior,dc=occourts,dc=org” This allowed the AOC to determine what IdP was being used in the authentication process. They would substring the user “cn=jsmith” and the IdP reference “cn=users,dc=ocsuperior,dc=occourts,dc=org.” Even though this approach allowed us to create a successful SAML solution, we are anxiously waiting for Oracle to develop an SP Identity Management product that can make policy decisions on the AttributeStatement being returned from the IDP.

The AOC installed WebLogic 11g on their own server. They followed our instructions on setting up an SP from our Phase I SP installation guide. We advised them to ignore the OES (Oracle Entitlement Server) section in the document and that the SP installation should work. Once everything was configured, we swapped Metadata to create a Circle of Trust. At this point, we were almost ready to test.

We had to setup firewall rules to allow our servers to communicate with each other. The AOC goes through the County Data Center, and they are notorious for taking a week to set up a simple firewall rule. Since we knew this was going to take a long time, we had management work out an arrangement to give our firewall rule priority and have it done within hours. We created a bridge line for our Network team and the Data Center. Our lead GFIPM developer was asked to keep trying to connect while they made multiple firewall changes. After about an hour, we were connected both ways.

Since the firewall rules have been established and the servers were able to talk to each other, we were ready to test our first SAML 2.0 transaction. When they tried to access their test app deployed on WebLogic, their link would go to a blank screen. We tried various configuration settings until we found the culprit. They needed to add a SAML2 Authenticator to their Authentication Providers in the Security Realm. Once this was added, the URL would redirect to the IdP and display a logon screen. Once they tried to login, an error would display on their screen. The problem occurred because the incoming IdP’s IP was different than the one that was configured on the server tab in OIF. There is a SAML 2.0 security check that makes sure that the IdP’s IP in the metadata must match the actual IdP’s IP. The problem occurred because the DNS name (“oifserver1”) was configured in OIF but was not included in the IdP’s metadata. The reason we changed the IP was because we were going through a proxy server with a different IP. Once we worked out this issue, the AOC tried to logon again. Another error message displayed when the AOC tried to logon. The message stated that the user cannot login. The message was not specific enough to tell us what the problem was. After an hour of searching OID, we found out that the users are given a default policy to expire after 90 days. Once we changed the password on the users in OID, the logon screen accepted the credentials and the browser redirected back to the AOC’s application. At this point, we had a full working SAML 2.0 IdP and SP.

2.1 Summary

By demonstrating that Superior Court and the AOC were able to perform a secure SAML 2.0 IdP and SP, we developed confidence that we can start a full production setup for SAML 2.0. This technology should allow our organization to provide more services to other agencies through a Circle of Trust. It will no longer be an administration nightmare to manage identities for outside agencies. Now, we will be able connect them to our organization through a simple on-boarding process.

Oracle's OIF product is excellent for setting up a SAML 2.0 IdP and appears to support all of SAML 2.0’s features. Unfortunately for this phase of the project OIF is severely limited when used with WLS as the SP due to WLS SAML 2.0 Support shortcomings.

The same can be said for Oracle Entitlements Server (OES), an excellent product with support of both basic, coarse-grained (role-based) and complex fine-grained access control including export of XACML policies. But again, WLS makes the product nearly inaccessible without significant patches and customization.

If OIF could communicate with OES (without Weblogic) the Oracle products for IdP/SP would be ideal.

2.2 Scenarios

User Log In Test

1. User will enter SP URL
2. User is redirected to IdP
3. User will enter their Username and Password
4. SAML is generated and pushed to AOC
5. AOC validates x.509 certificate
6. User sees CCPOR application