Extending Identity and Access Management to iOS Mobile Devices

Sudhir Tadi
Oracle
Bangalore

Keywords:

OAM, OAAM, iOS, Mobile, Native Apps, SSO, Fraud Prevention

Introduction

This presentation brings Oracles Mobile & Social security architecture to life by walking us through a day in the life of a mobile technician and his iOS Device. It shows how Oracle's Identity and Access Management products extend security and protection out to mobile devices, with native iOS application single sign-on strong authentication and fraud detection. It includes single sign-on to the iOS browser application to access Oracle's WebCenter Portal applications and Simple HTML Application. We even find out what happens when our hapless technician loses his device.

Solution Architecture

Below diagram gives an overview of the components installed and the integrations among various components.We have weblogic as application server and Access Manager, Adaptive Access manager integration with Mobile and Social Sever. Oracle Unified Directory acts as a user identity store.OAM Webgate along with OHS registered with OAM. We have simple web application for the user registration which captures the security questions and answers.

The registration application is protected with OAAM basic authentication scheme. We have installed three Native Applications on the device among which one acts as SSO Agent and remaining two applications acts as the clients.

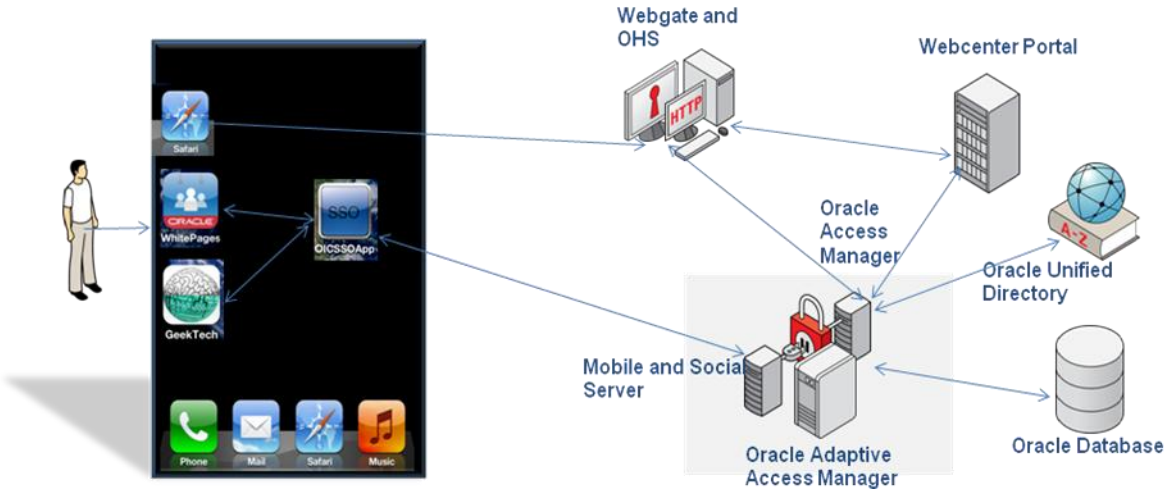
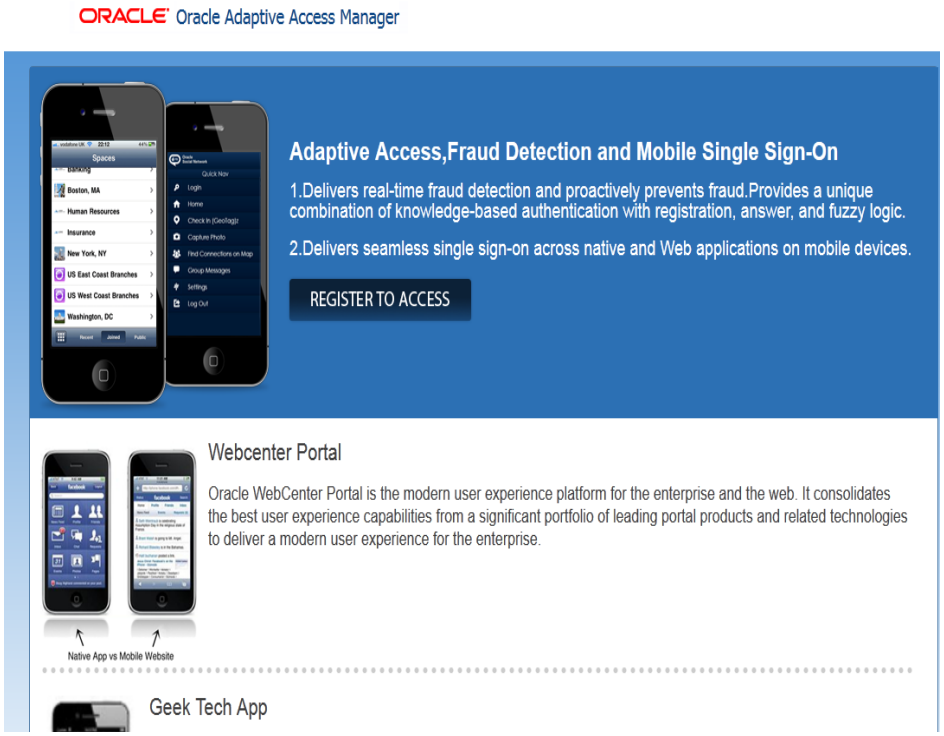


Illustration. 1: Architecture

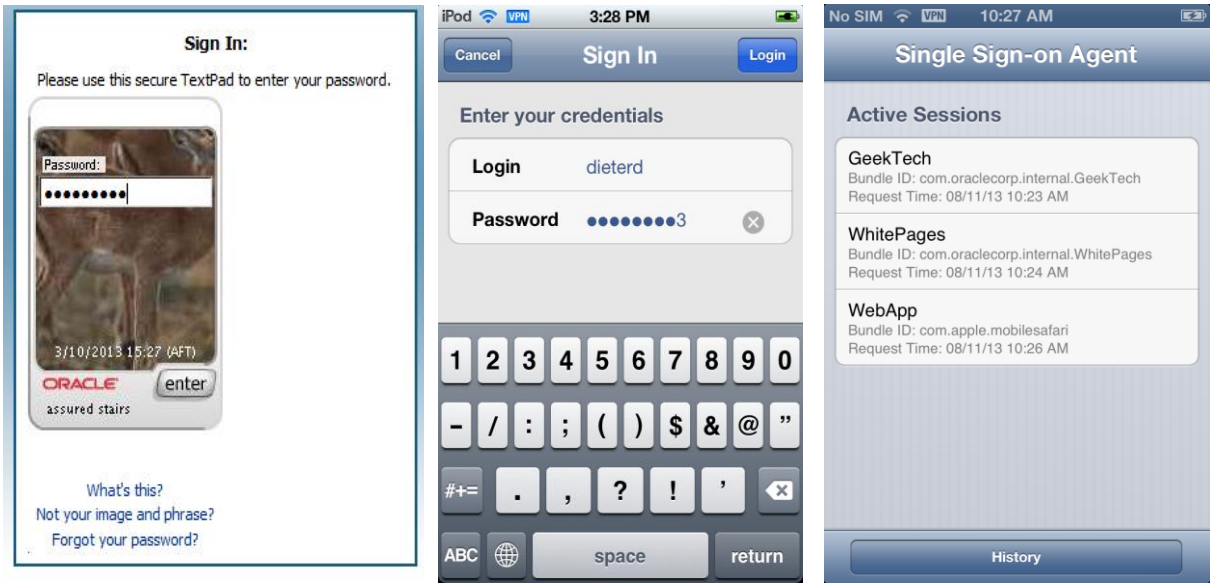
Usecases

The demonstration takes a look at the life of a mobile technician who uses a mobile device to assist him in his daily job of servicing technical products in the field. On his device he has 2 key native applications and, of course, a mobile browser. The first application is unfortunately named "GeekTech" and provides him with all the most common documentation he needs to assist in servicing and repairing appliances. As the story goes the new technician first registers himself, supplying passwords and challenge questions and answers.



This gives him access to the applications secured with OAM. To access the GeekTach application to view a service manual he must log on through OAM's mobile single sign on solution. A second challenge question is presented to our technician. This is because we have implemented OAAM and here we've established a few rules based on risks. In this case either the challenge comes because this is the first's time our newly registered user has accessed the application from this device.

Our technician finds that he doesn't have the latest manual and needs to call a colleague – he can do this by accessing a Whitepages native iOS application to find the subject matter expert. Switching to the native application we see that there is no sign on necessary. The expert tells our technician that there is a new manual that is currently being approved through their content management solution, Web Center Content. So, our technician switches to the mobile browser to find the new document.



The WebCenter Content application is secured but our use-cases shows that he is taken directly to the content without having to sign on. This is great – our technician has logged in once but the SSO solution has passed his credentials to the second native iOS application and also passed the credentials to the browser application too. A third native application deployed to the device allows us to see the 3 secure sessions that are running – this application has been built with the OAM Mobile software development kit (SDK).

All good so far and a nice story of extending the company's security out to mobile devices. The next part of the story describes how our hapless technician loses his mobile device along with a piece of paper taped to it with the password written down. Not clever. But no problem since we can block the device in the OAAM administration console and add the device to the block list.

Contact address:

Sudhir Tadi
Oracle
Tower D, IBC Knowledge Park, Bannergatta Road,
560076, Bangalore

Phone: +91.80.4029.2595
Email sudhir.tadi@oracle.com