Real-world Single Sign-On mit ADF Faces und OFM 11g

Olaf Heimburger
Oracle Deutschland B.V. & Co. KG
Berlin

Schlüsselworte:

Fusion Middleware, Oracle AS Single Sign-On, Oracle Access Manager, ADF Faces, ADF Security

Einleitung

ADF Faces Anwendungen zu sichern kann, je nach Anforderungen, einfach, aber auch sehr komplex werden. End-to-end Security scheint noch schwerer zu sein. Bei der Arbeit mit unseren Kunden entdeckten wir viele verschiedene Ansätze um auf allen Ebenen ein Single Sign-On zu erreichen. Single Sign-On mit Oracle AS Single Sign-On oder Oracle Access Manager Single Sign-On sind lediglich die ersten Hürden die man nehmen muss.

Single Sign-On Lösungen

Für jede Anwendung ist es erforderlich die Anwender zu kennen (authentifizieren) und ihnen die passenden Aufgaben zu erlauben (autorisieren). Die Landschaft der möglichen Single Sign-on Lösungen ist schier unübersichtlich und nicht jede ist für jeden Einsatz geeignet. Die möglichen Kandidaten werden nachfolgend kurz erläutert.

OpenID, GoogleID, Yahoo!ID

Die “Standards” OpenID, GoogleID, Yahoo!ID und andere sind als fremde Lösungen zu betrachten. Sie werden zum Teil von großen, weltweit verfügbaren Anbeitern zur Verfügung gestellt und versprechen eine einheitliche und jederzeit verfügbare Lösung. Obwohl Microsoft mit Passport einigen Schiffbruch erlitten hat, scheuen sich die anderen Anbieter nicht es „besser zu machen“. Im wesentlichen beschränken sich diese Anwendungen auf die Autorisierung des Benutzers für den Zugang eines angebotenen Webdienstes.
War bei Microsoft Passport der Vorbehalt wegen der möglichen missbräuchlichen Nutzung noch sehr hoch, hat sich das Bild bei Google oder Yahoo! erstaunlicherweise geändert. Obwohl die Verwendung der gesammelten Daten bei diesen Anbieter genauso unklar ist, ist die Bereitschaft diese Dienste einzusetzen bedeutend höher.

Windows Native Authentication (WNA)

In einem Unternehmensnetzwerk mit Windows Domain Servern, in der Regel mit Microsoft Active Directory implementiert, haben wir es hier mit einer verbreitenden Lösung zu tun. Im wesentlichen meldet man sich an seinem Arbeitsplatz an und kann entsprechend konfigurierte Anwendungen wie Outlook ohne weitere Anmeldung verwenden. Der Einsatz von Web-Anwendungen kann durch geeignete Konfiguration, besonders einfach mit dem Microsoft Internet Information Server, der gleiche Effekt erzielt werden.

Kerberos/SPNEGO

Mit Kerberos steht eine vom MIT entwickelte, plattformunabhängige Single Sign-on Lösung zur Verfügung. Nahezu jede verfügbare Plattform ist mit der entsprechenden Implementierungen ausgestattet und kann durch gezielte Konfiguration für diesen Dienst eingerichtet werden („kerberized“). Selbst exotische Anwendungen wie die Oracle Datenbank können für diesen Dienst konfiguriert und entsprechend verwendet werden (siehe auch DOAG News 3/2010).

Oracle AS Single Sign-On

Mit Oracle AS 9.0.2 wurde eine offene Single Sign-on Lösung für Web-Anwendungen eingeführt. Offen meint hier, dass ein Mechanismus zur Authentifizierung zur Verfügung gestellt wird. Ob dieser Mechanismus genutzt werden soll und wie die Autorisierung der Anwender der registrierten Anwendungen vorgenommen werden soll, bleibt Aufgabe der Anwendung. Natürlich sind mehrere Lösungen mit mehr oder weniger identischen Lösungen, auch im gleichen Unternehmen, die Folge.

Oracle Access Manager Single Sign-On

Der Nachfolger für Oracle AS Single Sign-On ist der Oracle Access Manager (OAM). Anders als das Oracle AS Single Sign-On übernimmt der OAM die Authentifizierung und Autorisierung der einzelnen Anwendungsteile. Er ist dabei nicht nur auf Web-Anwendungen beschränkt, sondern kann sich bei vielfältigen Anwendungen einklinken. Mit dem OAM werden Authentifizierungen und Autorisierungen zentral und für die Anwendungen transparent verwaltet.

SAML

Mit der *Security Assertion Markup Language* (SAML) steht ein Standard zur Verfügung, der unternehmensübergreifende Single Sign-On Lösungen unterstützt. Der sowohl Web-Anwendungen aber auch SOA-Anwendungen unterstützt. Die Kernidee ist die Implementierung zweier Typen von Anbietern (Provider) die entweder Dienste (Service Provider) oder Identitäten (Identity Provider) zur Verfügung stellen. *Service Provider* und *Identity Provider* können zu unterschiedlichen Einheiten eines Unternehmens oder sogar befreundeten Unternehmen gehören und durch gegenseitiges Vertrauen (Circle of Trust) die passenden Anwendungen für die Anwender authentifizieren und autorisieren. SAML stellt damit einen wesentlichen Standard für moderne SOA-basierte Anwendungen zur Verfügung. Passende Infrastrukturen können u.a. mit Oracle Identity Federation implementiert werden.

Welche Option sollte gewählt werden?

Die Auswahl des Single Sign-On Systems muss genau abgewogen werden. Sollen die Identitäten durchgängig auf allen Ebenen der Anwendung verwendet werden, kommt lediglich eine Lösung in Frage, die möglichst flexibel und von allen Ebenen eingesetzt werden kann. Besonders hervorzuheben ist hier die Einbindung eines LDAP-Verzeichnisses für alle erlaubten Identitäten. Lösungen wie WNA, Kerberos, Oracle Access Manager oder SAML spielen hier eine Rolle.

Populäre Lösungen wie OpenID, GoogleID oder Yahoo!ID haben ihren Reiz, sind aber bei genauer Betrachtung als eher gefährlich einzuordnen. GoogleID und Yahoo!ID lagern den Identitätsspeicher aus und können nicht ohne weiteres auf allen Ebenen, zum Beispiel der Datenbank, integriert werden. OpenID ist sogar noch fragwürdiger, da im Prinzip jeder Anwender einen eigenen OpenID-Authorisierungsserver betreiben und damit unkontrollierten Zugriff auf sensible Unternehmensdaten erhalten kann.

So weit so gut!

Moderne Anwendungsarchitekturen bestehen aus mehreren Schichten und Komponenten. In der Regel kann man von einem grafischen Schnittstelle (GUI) zur Interaktion mit dem Anwender ausgehen. Dahinter wird es aber sehr spannend. Die einfachste Variante ist ein direkter Zugriff auf eine eingebettete Datenbank. Soll die Anwendung von mehreren Anwendern gleichzeitig genutzt werden, gibt es eine zentrale Datenbank (zum Beispiel als Client-Server Anwendung). Und wird die Anwendung nicht mehr auf dem Arbeitsplatz installiert kommt noch die oder andere Middleware-Schicht hinzu. Mit dem Aufkommen von SOA wurde diese Middleware-Schicht um weitere Komponenten erweitert, deren Tiefe und Komplexität nicht einmal im Ansatz zu erkennen ist, da eine vernüftige Implementierung genau diese verbirgt.

Angemeldet, und nun?

Als Anwender ist man zufrieden, wenn man mit der gewünschten Anwendung und den erforderlichen Funktionen arbeiten darf. Richtig glücklich ist man aber, wenn die bearbeiteten Daten nicht verfälscht werden und die Integrität und Vertraulichkeit gewährleistet ist. Aus Sicht des Betreibers ist es erforderlich alle Maßnahmen zu treffen um diese Integrität und Vertraulichkeit zu garantieren und nachweisen zu können, dass dies auch der Fall ist. Zu jeder Zeit! Dafür muss aber an jeder Stelle der Anwendung die Identität des Anwenders bekannt sein.

Bei einer einfachen Anwendung mit integrierter Datenbank ist dies leicht zu erreichen. Sobald aber schon eine Komponente von mehreren Anwendern, bewusst oder unbewusst, genutzt wird, muss dafür gesorgt werde, dass die Identität an jeder Stelle bekannt ist. Aus diesem Grunde, sollte keine Lösung eingesetzt werden die nicht mit einer zentralen Anwenderverwaltung, nach heutigem Standard ein LDAP-Verzeichnis, gekoppelt werden kann. Mit Hilfe dieses Verzeichnisses werden die Anwender in allen Ebenen bekannt gemacht und stehen dort zur Verfügung.

Single Sign-On Integration

Bei der Gestaltung einer ADF Anwendung spielt ADF Security eine wesentliche Rolle. ADF Secrity verwendet wiederum das Oracle Platform Security System (OPSS) als allgemeine Schicht zu beliebigen Quellen, die die im *Java Authentication and Authorization Service* (JAAS) Kontext erforderlichen Subject- und Principal-Objekte erstellen können. Als Ergebnis kann die Anwendung auf ein JAAS-Subject vertrauen und anhand diesem die Authentifizierung und Autorisierung der gewünschten Funktionalität ermitteln.

OPSS ist flexibel und modular aufgebaut und erlaubt die Integration beliebiger LoginModule, die helfen die notwendigen Subjects und Principals zu erstellen. In Kombination mit dem Oracle Web Service Manager erlaubt OPSS die Identitäten zwischen verschiedenen Schichten in der Anwendung, aber auch an externe Anwendungen weiterzuleiten, ohne dass der Anwender sich erneut anmelden muss.

Beispielanwendung

In der vorgestellten Beispielanwendung wird gezeigt, wie eine ADF Faces Anwendung mit Oracle Access Manager integriert werden kann, um einen flexiblen und sicheren Zugang zu dieser Anwendung zu implementieren.

Kontaktadresse:

Olaf Heimburger
Oracle Deutschland B.V. & Co. KG
Schloßstr. 2
D-13507 Berlin

Telefon:	+49 (0) 30 435 795-160
Fax:	+49 (0) 30 435 795-419
E-Mail	olaf.heimburger@oracle.com
Internet:	blogs.oracle.com/olaf