Viele geschäftskritische Applikationen verwenden eine programmatische (nicht-deklarative) Zugriffssteuerung. Obwohl Informationen wie „Mitarbeiter X ist in der Gruppe G" in externen Verzeichnissen abgelegt sind, werden die Möglichkeiten verfügbarer Standards wie LDAP, XACML, RBAC oder JAAS nur wenig genutzt. Dies führt im günstigsten Fall zu höheren Kosten – insbesondere im Bereich der Wartung. Im ungünstigsten Fall kann eine programmatische Zugriffssteuerung zu unberechtigten Zugriffen führen. Der Artikel stellt den Oracle Entitlement Server (OES) vor und beschreibt, wie man damit eine wartungsfreundlichere, flexiblere Zugriffssteuerung erreicht.

Secure your code, don´t write security code!

Abdi Mohammadi und Heike Jürgensen, ORACLE Deutschland B.V. & Co. KG

Um eine Zugriffsregel wie „Als vertraulich markierte Dokumente dürfen nur von Mitarbeitern des Personalbüros von 8 bis 17 Uhr und nur innerhalb des Firmennetzes abgerufen werden" zu implementieren, gibt es zwei Möglichkeiten:

- *Variante A (programmatische Sicherheit)*
  Die entsprechende Applikation (z.B. ein Dokument-Managementsystem) enthält Programmcode, der genau diese Regel implementiert:

```
Boolean checkAccess (Date
date, Document doc, In-
et4Address sourceIP, Principal
user)
{if (isInRole(user, „Personal-
buero") && sourceIP.isLocal()
&& date.inWorkingHours {...}
                ....

}
```

  Die Überprüfung, ob der Nutzer in einer Gruppe/Rolle ist (isInRole) erfolgt zumeist durch eine LDAP/ Directory-Abfrage. Dies reicht aber nicht aus, um die erwünschte Flexibilität zu erreichen.
- *Variante B (deklarative Sicherheit)*
  Die entsprechende Applikation (etwa ein Dokument-Managementsystem) enthält selbst nicht mehr die Logik (obiges IF-Konstrukt), sondern fragt bei einem externen System nach. Hier ist die Funktionalität „checkAccess" außerhalb der geschäftskritischen Applikation implementiert. Der Methodenaufruf selbst erfolgt von derselben Stelle aus wie bei Variante A.

Der Ansatz, die Entscheidung darüber, ob ein Zugriff gewährt werden darf oder nicht, vollständig auszulagern – und nur eine Ja/Nein-Antwort zurückzuerhalten –, bietet folgende Vorteile:

- Besseres Sicherheitsmanagement: Falls sich die Regel ändert, muss die Applikation nicht geändert werden
- Flexiblere Architektur: Ein externes System, das Zugriffsentscheidungen trifft, kann von mehreren Geschäftsanwendungen gleichzeitig benutzt werden
- Unternehmensverantwortliche Personen (wie der Sicherheitsverantwortliche) können ihren Aufgaben nachgehen und die Regeln verändern, ohne komplizierte Abstimmungsgespräche mit den Anwendungsentwicklern zu führen

Darüber hinaus kann ein externes System mehr Funktionalität wie Mandantenfähigkeit und delegierte Administration bieten. Dies sind Eigenschaften, die in den seltensten Fällen in die anwendungsinternen Zugriffssteuerungsmodule implementiert werden. Die Vorteile sind, wie üblich in solchen Bereichen:

- Niedrigere Kosten, sofern es mehr als eine Geschäftsanwendung gibt, die ein solches externes System nutzt
- Höhere Sicherheit durch eine übersichtlichere Managebarkeit

Mit dem Übergang von programmatischer zu deklarativer Sicherheit sind auch initiale Kosten und technische Herausforderungen verbunden.

Oracle Entitlement Server

Der Entitlement Server bietet einen Administrations-Server, auf dem die Policies zentral verwaltet und in einer zentralen Datenbank gespeichert sind. Diese Regeln können über eine mitgelieferte Oberfläche gepflegt werden. Die Autorisierungs-Engines (Security Module oder „SM") fungieren dann als Policy-Decision-Point (PDP) und können entweder in die Applikation eingebettet (Embedded SM) oder zentral installiert sein. Der Autorisierungs-Server kann über unterschiedliche Protokolle wie XACML, RBAC, RMI etc. kommunizieren. Diese Ansätze können auch gemeinsam eingeführt werden, je nach gewünschter Ausrichtung. Der Embedded-Ansatz kommt beispielsweise im Portal-Umfeld häufig vor, da hier die Autorisierungsregeln selten geändert und eine hohe Anzahl von Berechtigungsanfragen innerhalb weniger Millisekunden durch die im Cache des Security-Moduls liegenden Informationen beantwortet werden. Das zentrale Deployment der Security-Module wird meistens gewählt, wenn die Autorisierungsregeln für mehrere Applikationen in einer heterogenen Infrastruktur gelten, Standard-Abfrageprotokolle wie XACML oder RBAC aus der Applikation heraus verwendet werden sowie die Antwortzeiten bedingt

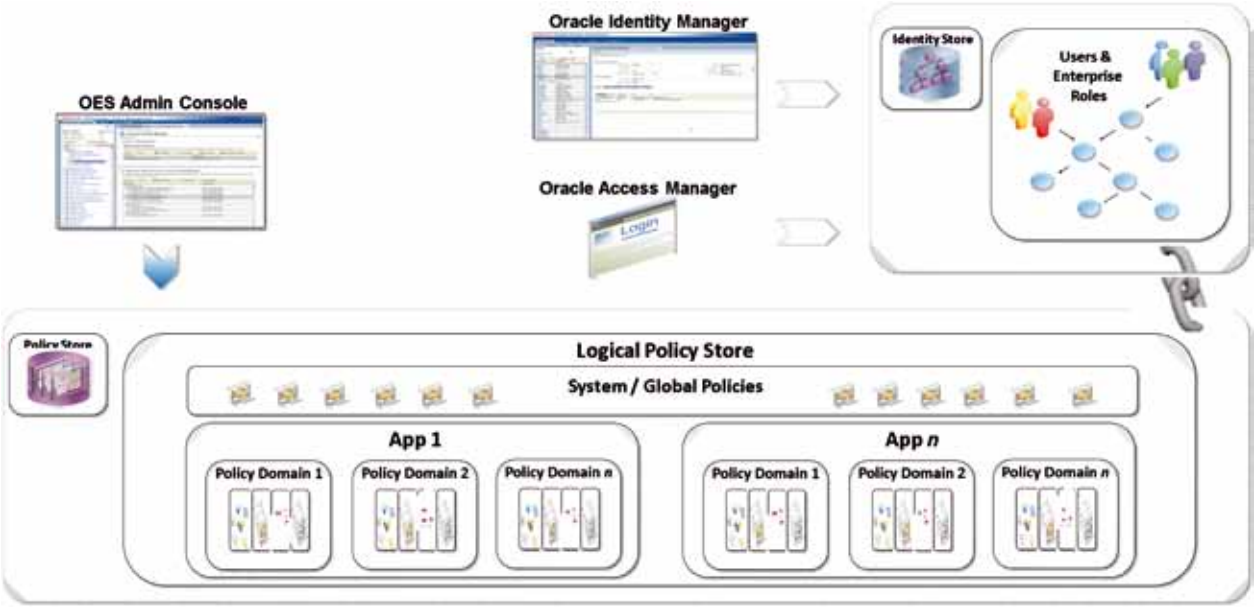

Abbildung 1: Zentrale Administration aller Applikations-Policies in unterschiedlichen Policy Domains

durch Netzwerk-Latenzzeiten keinen kritischen Aspekt darstellen (siehe Abbildung 1).

Die Entitlement-Server-Architektur

Abbildung 2 zeigt die unterschiedlichen Komponenten sowie die logischen Schnittstellen der Entitlement-Server-Architektur. Die linke Seite bildet die mögliche Überprüfungs-Architektur ab: integriert (embedded) oder zentral. Die rechte Seite zeigt die Schnittstellen, um die Administration des Oracle Entitlement Servers außerhalb der Administrationsoberfläche zu ermöglichen.

Der Administrations-Server (Policy Administration Point, PAP) wird in einem Application-Server wie dem Oracle WebLogic Server eingerichtet und bietet die grafische Oberfläche zum Erstellen von Policies, die später den Applikationen zugewiesen und über die Autorisierungs-Engine zur Laufzeit geprüft werden. Die untere Ebene der Abbildung spiegelt die Möglichkeiten der Schnittstellen der Autorisierungs-Engine wider. Die erstellten Policies sind in dem OES-Policy-Store abgelegt. Die notwendigen Attribute und Anwenderinformationen für die granulare Autorisierung können auch aus externen Directory-Servern zur Applikationslaufzeit verwendet werden. Dadurch ist eine Wiederverwendbarkeit von bereits definierten Berechtigungs-Informationen wie definierten LDAP-Gruppen in einem bereits vorhandenen Directory-Server beim Ausbau eines zentralen Autorisierungsdienstes mit dem Entitlement Server möglich (siehe Abbildung 3). Beim Erstellen von Policies wird in der Regel Folgendes festgelegt:

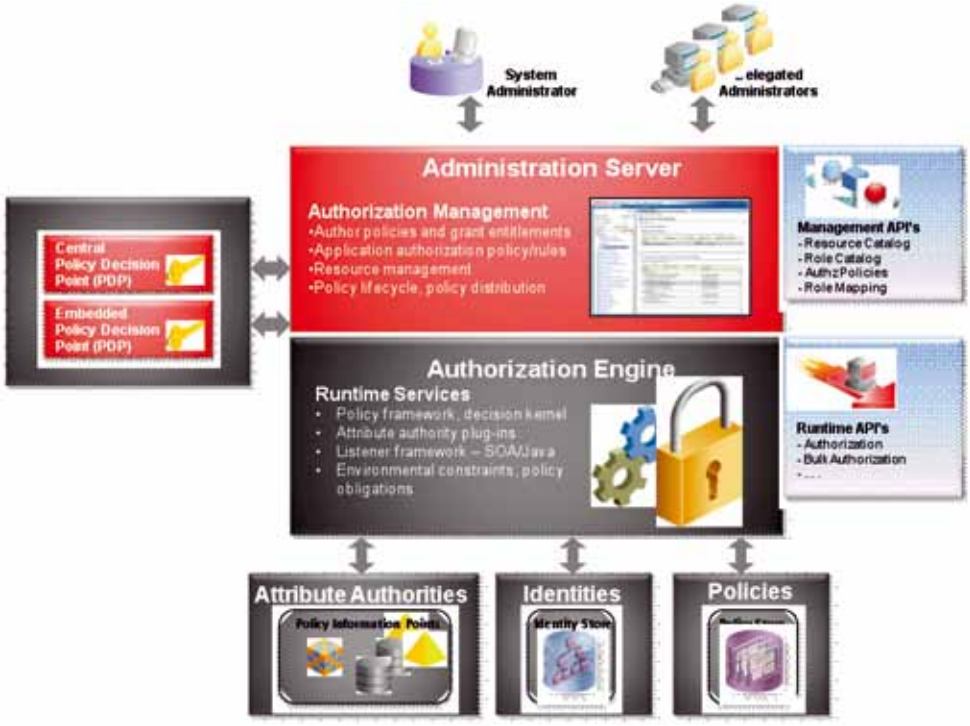

Abbildung 2: Funktionale Entitlement-Server-Architektur

- Wer (Principal)
- Unter welchen Rahmenbedingungen (Constraints)
- Worauf (Ressource)
- Mit welchen Aktivitäten (Action)
- Kontrolliert zugreifen darf (Effect)

Beispielsweise dürfen Dokumente mit dem Vermerk „vertraulich“ nur von

Mitarbeitern des Personalbüros von 8 bis 17 Uhr und nur innerhalb des Firmennetzes abgerufen beziehungsweise bearbeitet werden.

Der Entitlement Server bietet „out-of-the-box" Security-Module wie für den Oracle WebLogic Server, Microsoft Sharepoint, Oracle Enterprise Gateway, die Oracle-Datenbank sowie für andere Applikationen und Datenbanken. Diese Systeme werden mit vordefinierten Policy Enforcement Points (PEP) wie auch mit Policy Decision Points (PDP) unterstützt. Um eigene Security-Module (integriert oder zentral) für Java- oder .Net-Umgebungen zu entwickeln, stellt Oracle entsprechende Schnittstellen und Bibliotheken zur Verfügung.

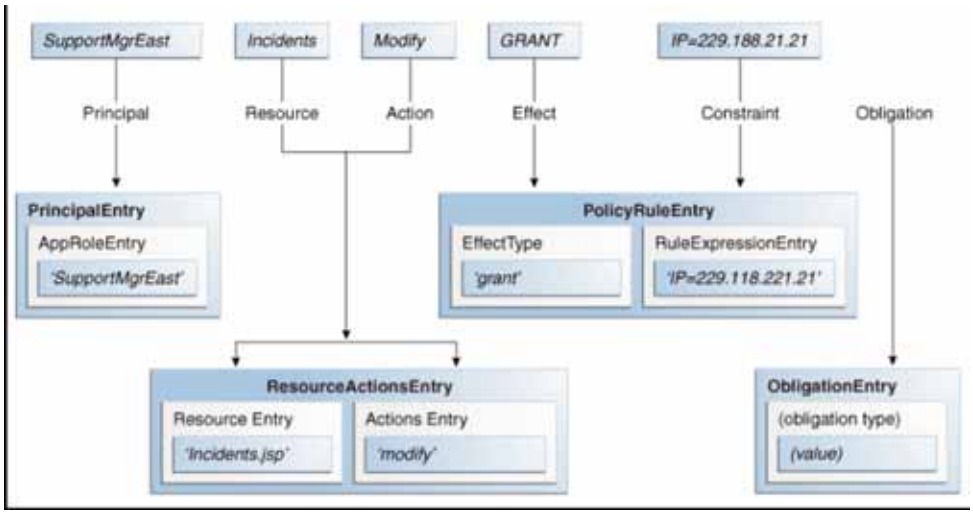

Abbildung 3: Logisches, fein granulares Berechtigungskonzept

Abbildung 4 zeigt eine Architektur mit einem zentralen Administrations-Server, der auf ein zentrales Policy-Repository und entsprechende Identity-Stores zugreift. Die Security-Module (integriert und/oder zentral) erhalten die aktualisierten Policies entweder periodisch oder interaktiv bei Änderungen des Administrations-Servers (Push-Methode). Sie können auch so konfiguriert werden, dass sie sich die Policies selbst abholen (Pull-Methode). Letzteres ist erforderlich, wenn beispielsweise das Security-Modul in der Demilitarized Zone (DMZ) steht und die Firewall-Regeln die Push-Methode vom Administrations-Server zum Security-Modul nicht erlauben.

Entitlement-Server-Oberfläche

Die grafische Administrationsoberfläche bietet die Möglichkeit, sämtliche Policies zu definieren und den Security-Modulen bereitzustellen (siehe Abbildung 5). Ausgehend von einer Applikation („Hello World" in Abbildung 3) können unterschiedliche Ressource-Typen wie verschiedene Seiten eines Portals definiert werden. Damit ist eine Kategorie für alle ähnlich funktionierenden Ressourcen (etwa bestimmte Unterfunktionen eines Web-Services) festgelegt. Die zu schützende Ressource, die relevanten Rollen und entsprechende Policies sind verein-

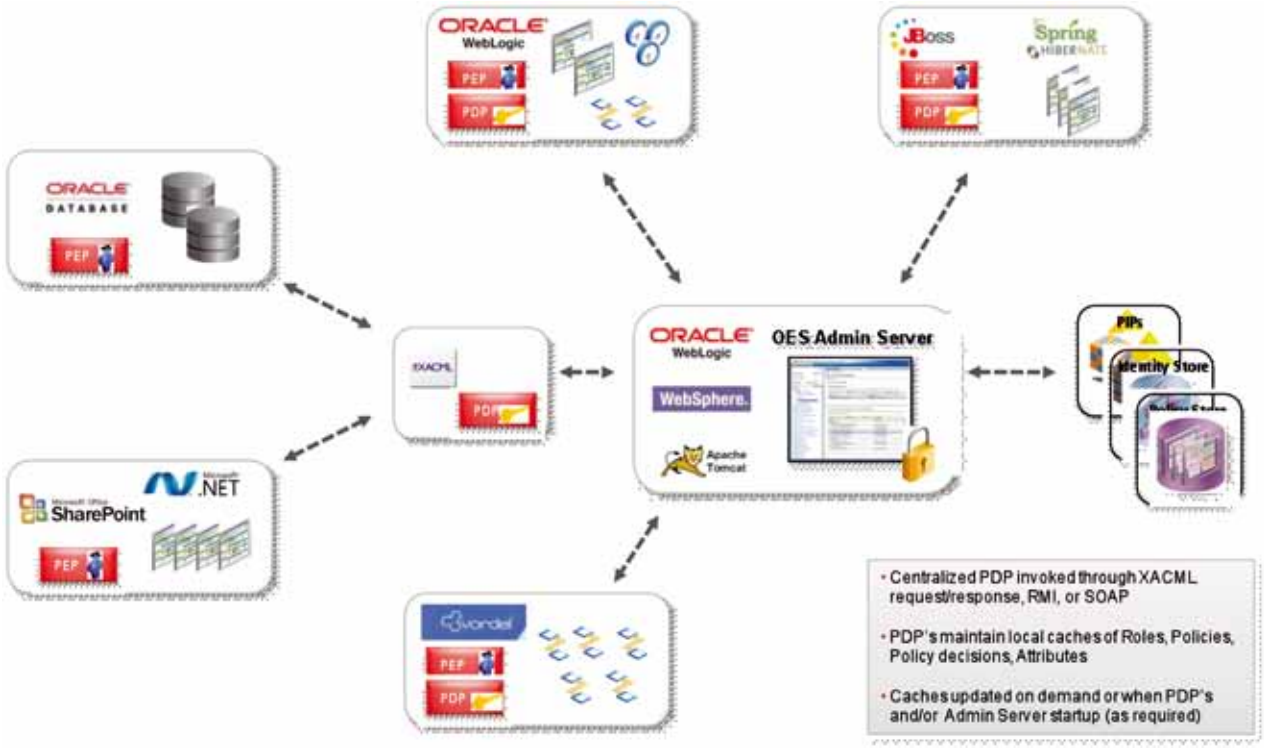

Abbildung 4: Security-Module mit zentraler Entitlement-Server-Architektur

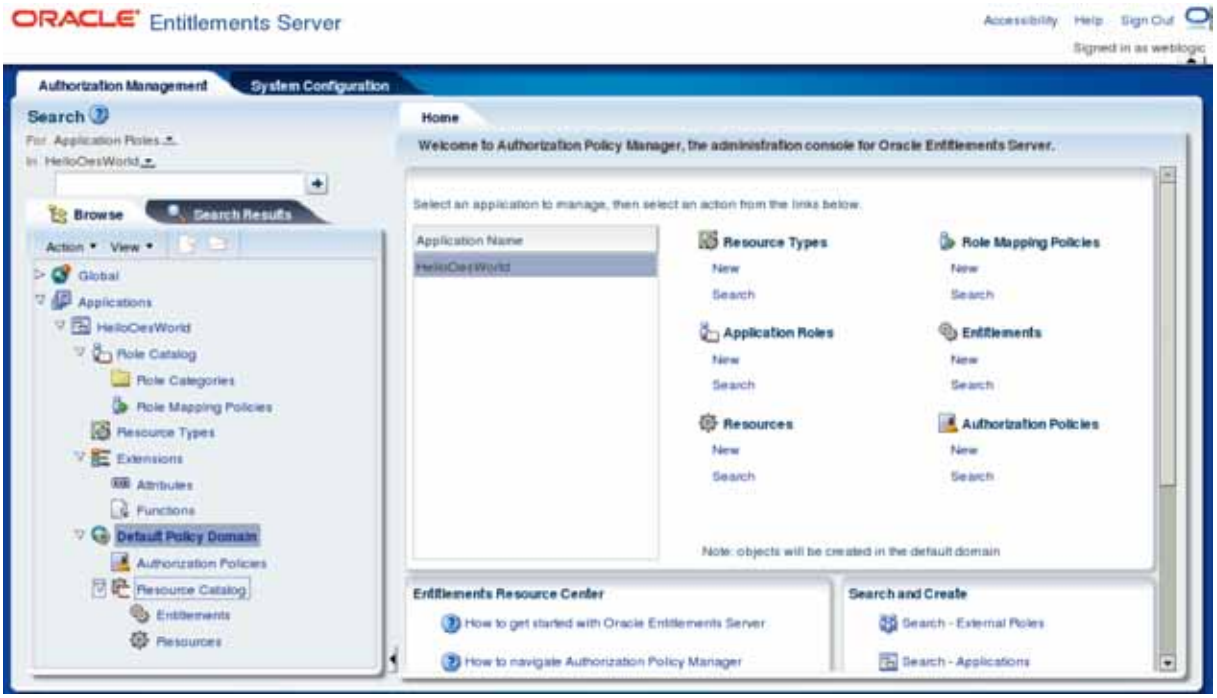

Abbildung 5: Administrationsoberfläche des Entitlement Servers

bart. Eine Gruppe von Ressourcen lässt sich als ein Entitlement zusammenfassen. Einer Ressource oder einem Entitlement werden dann eine oder mehrere Autorisierungs-Policies zugewiesen. Beispielsweise kann einem neuen Mitarbeiter einer Abteilung mit einer einzigen Policy ein Entitlement zugewiesen werden, das ihm den Zugriff auf das Intranet-Portal, das Telefonbuch und auf einige Standard-Dokumente erlaubt.

Einsatzmöglichkeiten

Der Entitlement Server wird immer dann seine Einsatzberechtigung haben, wenn nicht nur der allgemeine Zugriff auf eine Ressource (URL, Web-Service) geschützt wird, sondern detaillierte Berechtigungen – Oracle spricht hier von feingranularen Autorisierungen – definiert werden müssen. Mit dem Entitlement Server kann einem Benutzer oder einer Applikation die Berechtigung für eine bestimmte Unterfunktion einer Anwendung erteilt oder verweigert werden. Beispielsweise lässt sich bei einem Zugriff auf eine Portal-Seite abhängig von definierten Policies steuern, dass nur bestimmte Informationen sichtbar sein sollen oder bei einer finanziellen Transaktion (Homebanking) maximale Beträge abhängig von Randbedingungen (Alter, IP-Adresse, Kontostand etc.) überwiesen werden dürfen. Bei medizinischen Einrichtungen möchte der behandelnde Arzt beispielsweise nur die Röntgenbilder einer anderen Klinik oder anderen Ärzten zur Zweitansicht erlauben. Durch den Entitlement-Server kann dann der Teil der Patientenakte als eine Ressource definiert und der Zugriff darauf mittels entsprechender Autorisierungsregeln eingeschränkt werden. In einer SOA-Umgebung können die unterschiedlichen Funktionen eines Web-Service-Providers mit Policies versehen werden, um Sicherheitskriterien für unterschiedliche Service-Consumer festzulegen.

Fazit

Durch den Einsatz des Oracle Entitlement Servers ist durch die konsequente Trennung von Security- und Applikations-Code eine leichtere und nach Bedarf konfigurierbare Security-Policy etabliert, die die Entwicklungskosten reduziert. Darüber hinaus wird vermieden, dass unterschiedliche Applikationen ihre eigenen Policies im Code festlegen und es dadurch zu widersprüchlichen Berechtigungen kommen kann. Ebenso wird die Wiederverwendbarkeit von applikationsweiten Rechtekonzepten ermöglicht und ein unternehmensweites Konzept sukzessive erreicht. Die Betrachtung auf die gesamte IT-Sicherheit kann wesentlich erhöht werden, sie wird transparenter und kontrollierbarer.

Durch das zentrale Autorisierungs-Management, das Monitoring von Änderungen sowie das Logging und Auditing von Zugriffen können ebenfalls bestehende Regularien erfüllt werden. Mit dem Entitlement Server lässt sich eindeutig feststellen, wer wann auf was zugegriffen hat und wer es ihm wann erlaubt hat.

Abdi Mohammadi
ORACLE Deutschland B.V. & Co. KG
abdi.mohammadi@oracle.com