Aufbau einer Sicherheitsarchitektur zum Schutz von Services

Markus Lohn
ORACLE Deutschland B.V. & Co KG
Nürnberg

Schlüsselworte
SOA, Webservices, OWSM, Security

Einleitung

Mit dem Oracle Web Services Manager wird eine Komponente in der Fusion Middleware zur Verfügung gestellt, um Services abzusichern. Zunächst wird die grundlegende Arbeitsweise und Architektur des Web Service Managers vorgestellt, insbesondere das Zusammenspiel mit weiteren Sicherheitskomponenten der Fusion Middleware. Anhand eines konkreten Kundenbeispiels wird eine mögliche Sicherheitsarchitektur für Services mit dem OWSM aufgezeigt und erläutert.

Sicherheitsanforderungen

Das Thema Sicherheit ist bei der Implementierung und Bereitstellung von IT-Systemen immer zu betrachten. Vor allem mit der Etablierung von sozialen Netzwerken und Cloud-Diensten im Internet wird die Frage nach der Sicherheit öffentlich diskutiert und bewertet. Dabei sind die Fragestellungen eigentlich immer gleich:

- Darf eine bestimmte Identität auf bestimmte Daten zugreifen? Hat die Identität die erforderlichen Berechtigungen? (Authentifizierung und Authorisierung)
- Ist sichergestellt, daß die Daten nicht in unbefugte Hände gelangen können? (Vertraulichkeit)
- Kann eine Manipulation von Daten ausgeschloßen werden? (Integrität)
- Kann der Datenzugriff protokolliert und überwacht werden? (Auditierung)

Auch im Rahmen einer SOA-Architektur müßen diese Fragen beantwortet werden. Jedoch sind in einer SOA noch zusätzliche Aspekte zu betrachten, die eine große Herausforderung darstellen.

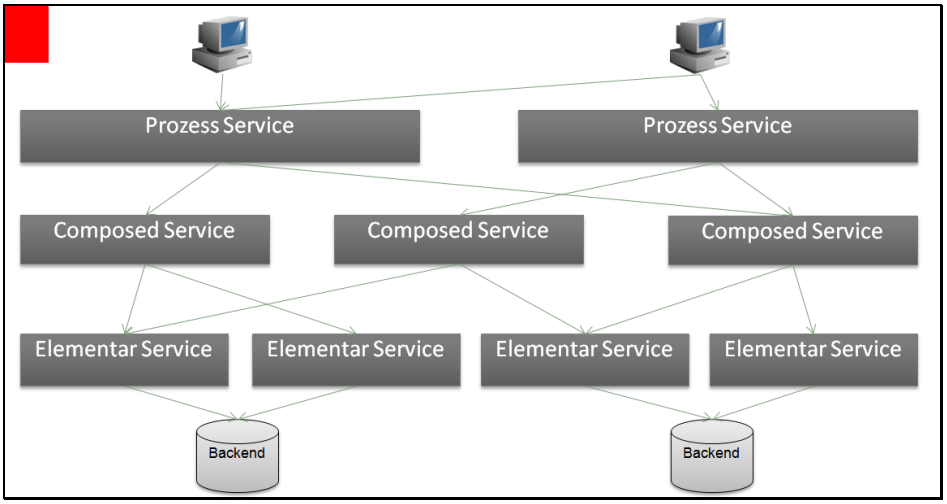

Abbildung 1 Kundenbeispiel für eine SOA Servicelandschaft

In einer SOA geht es typischerweise um das Verbinden und integrieren von verteilten Systemen. Es gibt eine Vielzahl von Services auf unterschiedlichen Abstraktionsebenen, wie in Abbildung 1 Kundenbeispiel für eine SOA Servicelandschaft dargestellt. Jedes System hat eigene Sicherheitsanforderungen und die Herausforderung ist, diese soweit in Einklang zu bringen, dass eine gemeinsame Sicherheitslösung realisiert werden kann. Spannend ist oft schon die Frage, wie Identitäten, z. B. Benutzer, in den einzelnen Systemen verwaltet werden oder an welchen Stellen eine Authentifikation und Authentifizierung durchgeführt werden muß. Dabei ist auch immer die Vertraulichkeit und Privatspähre zwischen den Systemen sicherzustellen. Auch das Thema Verschlüsselung muß betrachtet werden. Ist die Verschlüsselung auf dem Transportweg ausreichend oder muß der Inhalt der Nachrichten selbst auch verschlüsselt werden?

WS-Sicherheitsstandards
Eine SOA-Architektur wird heute häufig auf Basis von Webservices realisiert. Die Definition der Operationen und Nachrichtenformat erfolgt immer auf Basis von XML.

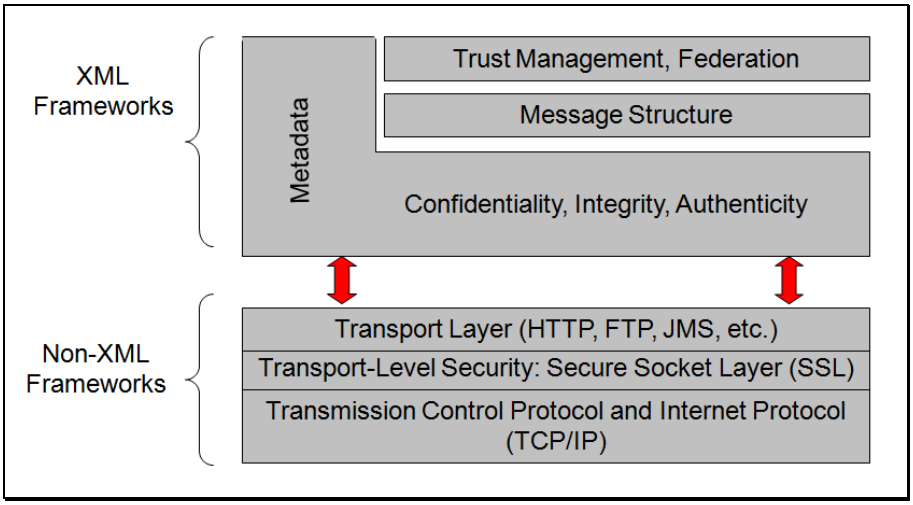

Abbildung 2 Security Standards und Frameworks

Aufbauend auf bereits etablierten Sicherheits-Algorithmen (RSA, AES, DES,...) und allgemeinen Sicherheitsstandards (SSL, X.500, PKI, Kerberos) gibt es deshalb eine Reihe von XML Sicherheitsstandards und zusätzlichen speziellen Sicherheitsstandards für Webservices:

- Confidentiality, Integrity, Authenticity
  - XML Encryption, XML Signature
- Message Structure, Message Security
  - SOAP, WS-Security
- Message Delivery
  - WS-Addressing
  - WS-Reliable Messaging
- Trust Management
  - SAML
  - WS-Trust
  - WS-Secure Conversation
- Metadata
  - WS-Policy, WS-Policy Attachment, WS-Security Policy
  - WS-Metadata Exchange
- Access Control
  - XACML

Wie zu erkennen ist, gibt es eine Vielzahl von Standards im Umfeld von XML und Webservices. Diese Standards liegen natürlich in unterschiedlichen Versionen vor und das fördert nicht unbedingt zu Interoperabilität, die ein wesentlicher Bestandteil in einer SOA ist. Ähnlich wie im Bereich der Webservices wurde auch für die Sicherheit ein sog. WS-I Basic Security Profile festgelegt. In diesem Profile werden Restriktionen in Bezug auf die Verwendung dieser Standards definiert. Hierdurch soll die Interoperabilität bei Nutzung dieser Sicherheitsstandards gewährleistet werden..

Oracle Web Service Manager Architektur (OWSM)

Für die Umsetzung von Sicherheitsanforderungen an Webservices in der Fusion Middleware (FMW) ist der OWSM vorgesehen. Er ist der Dreh- und Angelpunkt für alle Webservice- und SOA-Applikationen. Produkte wie der Oracle OSB oder Oracle SOA-Suite sind optimal mit dem OWSM integriert. Nachfolgend werden die wichtigsten Bestandteile der OWSM-Architektur kurz erläutert.

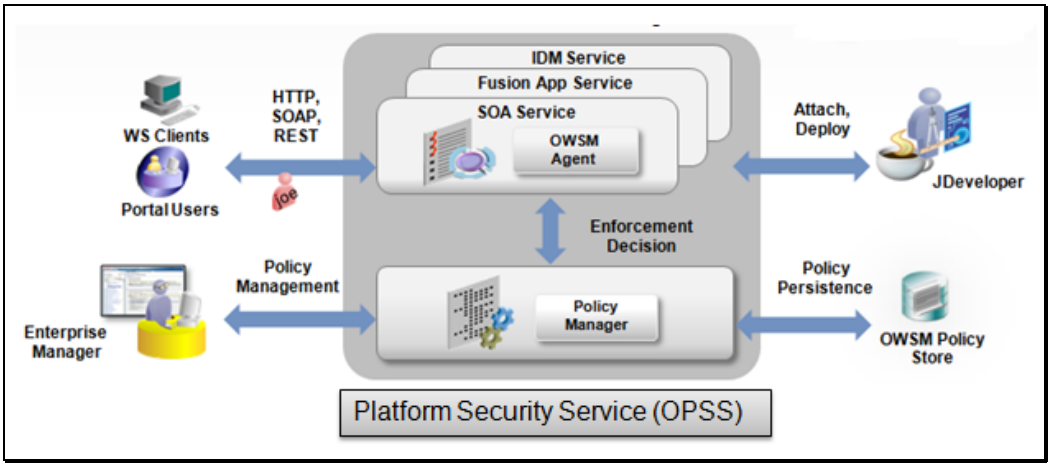

Abbildung 3 Architektur Oracle Web Service Manager

Policies und Policy Types
Die Sicherheitsanforderungen, die durch den OWSM geprüft und sichergestellt werden müßen, werden in Form von Policies definiert. Policies können in Kategorien unterteilt werden (sog. Policy Types). Zur Zeit stehen folgende Kategorien zur Verfügung: WS-Reliable Messaging, Management, WS-Adressing, Security und MTOM. Eine Policy wiederum besteht aus mind. einer Assertion. Eine Assertion stellt letztendlich eine Aktion dar, die auf den Request bzw. auf die Response angewandt werden. Assertions werden nacheinander in einer Kette (Pipeline) durchlaufen.
Es gibt eine Vielzahl von Policies die automatisch bei der Installation mitgeliefert werden. Jedoch besteht auch die Möglichkeit neue Policies zu definieren. In diesem Fall ist zu empfehlen, der vorgeschlagenen Namenskonvention für Policies zu folgen.

Das Zuweisen von Policies zu Services kann auf zwei Arten durchgeführt werden. Zum einen während der Entwicklungsumgebung, z. B. mit dem JDeveloper. Zum anderen automatisch durch die Definition von Policy Sets in der Runtime-Umgebung. In diesem Fall werden die Services nach der Installation automatisch durch das Hinzufügen der Policies geschützt. Der Entwickler muß sich somit nicht mehr um Sicherheitsaspekte kümmern und kann sich auf die Implementierung der fachlichen Anforderungen konzentrieren.

OWSM Agent

Der OWSM Agent ist dafür verantwortlich, den Zugriff auf geschützte Services zu überprüfen. Er erzwingt die Einhaltung von definierten Policies. Zu diesem Zweck kommuniziert er mit dem Policy Manager. Vom Policy Manager erhält der Agent alle notwendigen Policy-Definitionen. Der OWSM Agent implementiert einen lokalen In-Memory Cache für Policies. In definierbaren Abständen erfolgt ein Abgleich mit dem Policy Manager. Dabei ist zu beachten, das lediglich Änderungen ausgetauscht werden.

Policy Manager

Mit dem Policy Manager können alle Policies im Policy Store verwaltet werden. Das Frontend für die Verwaltung der Policies ist im Fusion Middleware Control integriert. Mit der Verwaltungsoberfläche können neue Policies angelegt, geändert, exportiert, importiert, etc.. werden. Die Policies selbst werden in Form von XML-Dateien in einer Datenbank gespeichert. Die Datenbank für den Policy Manager basiert auf dem sog. Master Data Services (MDS) Repository. Das MDS ist eine zentrale Komponente, die durch weitere FMW-Produkte zum Ablegen von Konfigurationseinstellungen oder anderen Artefakten genutzt wird.

Oracle Platform Security Service (OPSS)
OPSS stellt die Basisplatform für Sicherheitsaspekte für FMW-Produkte, z. B. WebLogic Server, SOA-Suite, OWSM, etc. zur Verfügung. OPSS abstrahiert von diversenen Sicherheits-implemetierungen und stellt API’s für den einfachen Zugriff bereit. Dies beinhaltet z. B. Verschlüsselungs-Algorithmen und Schlüssel-Management oder Zugriff auf Identitymanagement Systeme.

Kundenbeispiel: Sicherheitsarchitektur für Services auf Basis eines zentralen Policy Managers

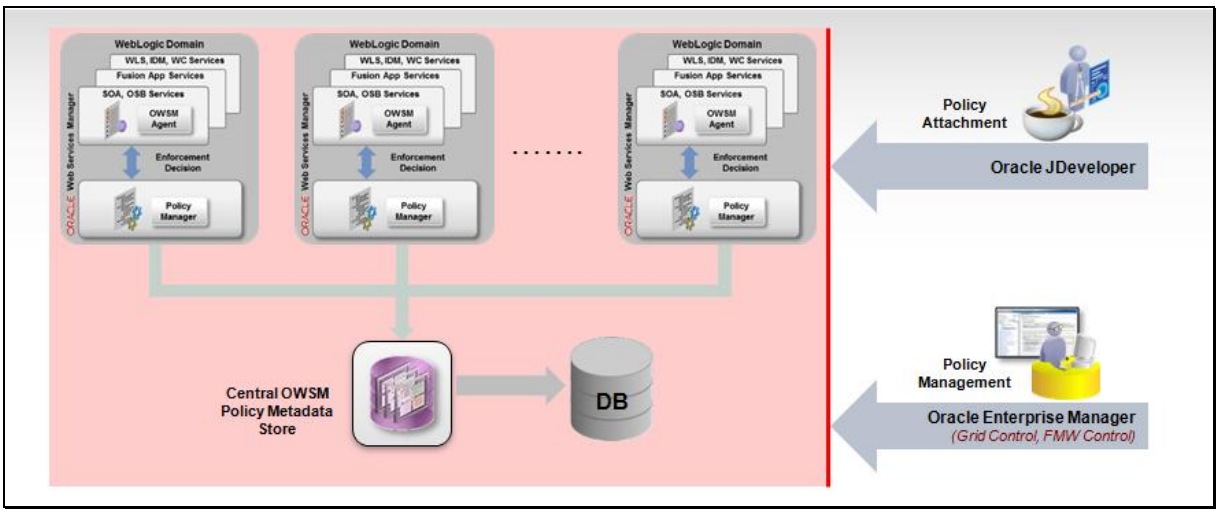

Abbildung 4 Deploymentarchitektur eines zentralen Policy Managers

Die Sicherheitsarchitektur für den Zugriff auf Services basiert auf einem zentralen Policy Manager. Aufgrund der hohen Anzahl an Umgebungen ist somit sichergestellt, das Änderungen an Policies zentral gepflegt und die Aktualität in den einzelnen Umgebungen sichergestellt ist. Hierzu existiert eine einzige, auf Hochverfügbarkeit ausgelegte, Weblogic-Domäne nur für die Bereitstellung des Policy Managers.

Für die Sicherstellung der Sicherheitsanforderungen hat der Kunde eigene Policies definiert und im OWSMS registriert. Die Policies werden in Form von Policy Sets automatisch bei der Installation den Services zugewiesen. Das Einrichtigen der Policy Sets erfolgt automatisch beim Aufsetzen der WebLogic Domänen.

Services dürfen nur durch eine authentifizierte Idendität aufgerufen werden. Die Identität muß als SAML Ticket zur Verfügung gestellt werden. Durch die eigenen Policy-Definitionen wird somit ein einheitliches Identity Propagation auf SAML Basis realisiert. Darüberhinaus ist der Kommunikationsweg für Services fest vorgegeben. Sichergestellt wird das durch Verteilung entsprechende Zertifikate und Definition von Trusted Client-Beziehungen im OWSM.

Fazit

Die Anforderungen an die Sicherheit von IT-Systemen sind im wesentlichen nicht neu. Jedoch gibt es im Rahmen einer SOA-Architektur eine Reihe von Herausforderungen, vor allem aufgrund der Heterogenität und Verteilung der Systeme, die zunächst einmal gelöst werden müßen. Darüberhinaus existieren in der Zwischenzeit eine Vielzahl von Sicherheitsstandards, vor allem Bereich XML, die insgesamt die Komplexität erhöhen.

Mit dem OWSM können viele Sicherheitsanforderungen sehr einfach durch Konfiguration und Deklaration gelöst werden. Jedoch ist zu beachten, daß man sich im Vorfeld umfassend mit dem Thema Sicherheit, im konkreten Anwendungsfall, auseinandergesetzt und die Anforderungen in einem Sicherheitskonzept verankert hat.

Kontaktadresse:
Markus Lohn
ORACLE Deutschland B.V & Co. KG
Lina-Ammon-Straße 19
D-90471 Nürnberg

Telefon:	+49 (0) 911-98182 461
Fax:	+49 (0) 911-98182 111
E-Mail	markus.lohn@oracle.com
Internet:	www.oracle.com/de