Identity Propagation in Fusion Middleware

Klaus Scherbach
Oracle Deutschland B.V. & Co. KG
Hamborner Str. 51, 40472 Düsseldorf

Schlüsselworte
Oracle Fusion Middleware, Oracle Access Management, Identity Propagation, Identity Context

Einleitung
Die Security Komponenten der Oracle Fusion Middleware ermöglichen eine durchgängige Verteilung der Nutzeridentität. Dieser Mechanismus reicht vom Web-Frontend bis tief in die SOA-Infrastruktur und kann auf vielfältige Weise genutzt werden: von Multi-Faktor-Authentifizierung über Web Single Sign-On und feingranulare Autorisierung bis zur gesicherten Übertragung der Nutzeridentität und zusätzlicher Nutzer- und Anmeldeinformationen bis ins Backend.

Beteiligte Komponenten sind Access Management (OAM/ OAAM), evtl. Webcenter, OWSM, OSB, OES.

Identity Propagation in Fusion Middleware
Die moderne, IT-gestützte Lebensweise weiter, insbesondere jüngerer Bevölkerungskreise stellt neue Anforderungen an IT-Infrastrukturen. Anwender wollen und können oftmals auch mit verschiedensten Geräten praktisch von jedem Ort der Erde aus auf Anwendungen zugreifen. Nicht jeder Zugriffsweg bietet ausreichende Sicherheit für jede Art von Anwendung oder Transaktion.

Daher muß erst einmal die Authentifizierung flexibel auf unterschiedlichste Umstände reagieren und im Zweifel stärkere Mechanismen zum Tragen bringen. Oracle Access Management verfügt über eine extrem anpassbare Authentifizierung; dazu einige Stichpunkte:

- pre/ post Authentication Rules zur dynamischen Verschaltung von Mechanismen
- neben den Standard-Mechanismen auch Social Login, Knowledge Based Authentication, One Time Paßworte, Time Based Mobile Authenticator
- Custom Plugin Framework

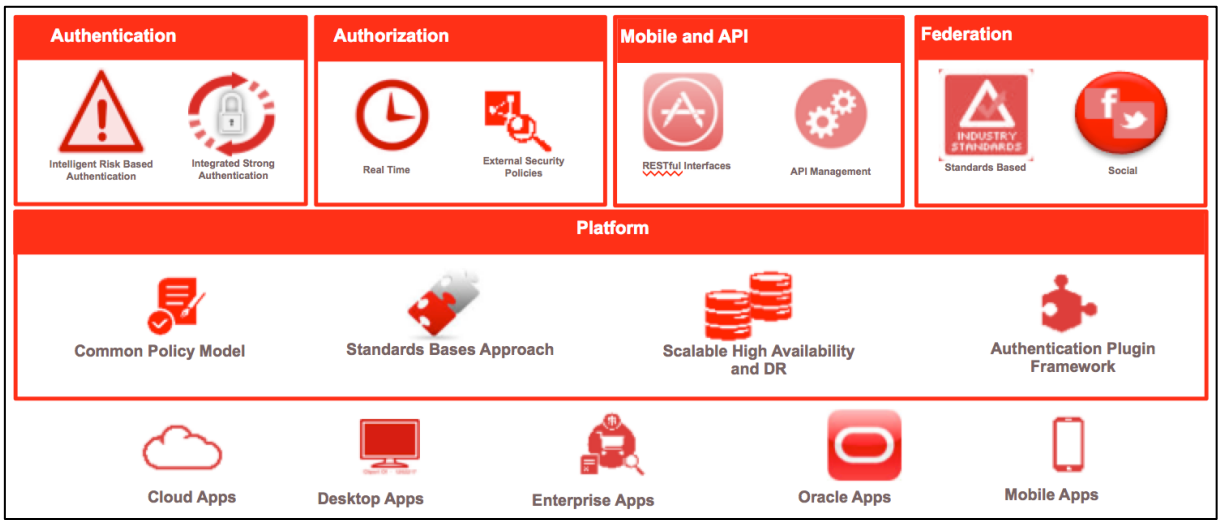

Abb. 1: Oracle Access Management Funktionalität

Die Art der Authentifizierung, zusätzliche Credentials des Nutzers sowie das erkannte Gerät und seine Einstellungen sowie etliche andere Faktoren bilden den „Identity Context“. Dieser Kontext kann zum einen dazu dienen, zusätzliche Authentifizierungsmechanismen zur Minderung des Risikos einzuschalten. Andererseits ist er die Grundlage für Autorisierungsentscheidungen auf unterschiedlichen Ebenen der IT-Infrastruktur.

Um hinsichtlich Autorisierung flexibel reagieren zu können, müssen nachgelagerte Komponenten aber zuverlässig über die Identität des Nutzers und den Kontext seines Zugriffs informiert werden. Dies geschieht mit Hilfe der in Oracle Fusion Middleware implementierten „Identity Propagation“ und „Identity Context“ Mechanismen. Identity Propagation erleichtert zudem durchgängiges Logging.

Die folgende Tabelle zeigt einige Beispiele für Attribute, die – je nach Konfiguration - im Identity Context eines Zugriffs verfügbar sein können.

Kategorie	Attribute	Publisher
Client	• Is Firewall Enabled • Is Anti Virus Enabled • Device Fingerprint • Location	OESSO OAM/ MS
Risk	• Is Known Device • Is Trusted Device • Risk Score	OAAM
Federation	• Partner ID • Partner Attributes	OAM/ OIF
Session	• Level of Assurance • Session ID • Any attribute in the current session	OAM
Identity	• Any attribute in the user’s ID Store profile • True/False result of a search	OAM OVD

Abb. 2: Beispiele für Identity Context Attribute

OAM Agenten fangen Zugriffe auf geschützte Anwendungen ab und fragen bei OAM hinsichtlich Authentifizierungs- und Autorisierungs-Entscheidung an (via OAP Backend-Protokoll). Nach erfolgter Authentifizierung überträgt der Agent mit dem Request zusätzliche Header an die integierte Anwendung. Dies sind im einfachsten Fall Klartext-Header, z.B. der OAM_REMOTE_USER Header mit der ID des authentifizierten Nutzers. Dies reicht als Basis für Single Sign-On und Identity Propagation bereits aus.

Identity Context jedoch erfordert eine kryptografisch gesicherte „Identity Assertion“. Basis ist ein SAML Token, das die Identität des Nutzers zusichert und auch zusätzliche Attribute umfassen kann.

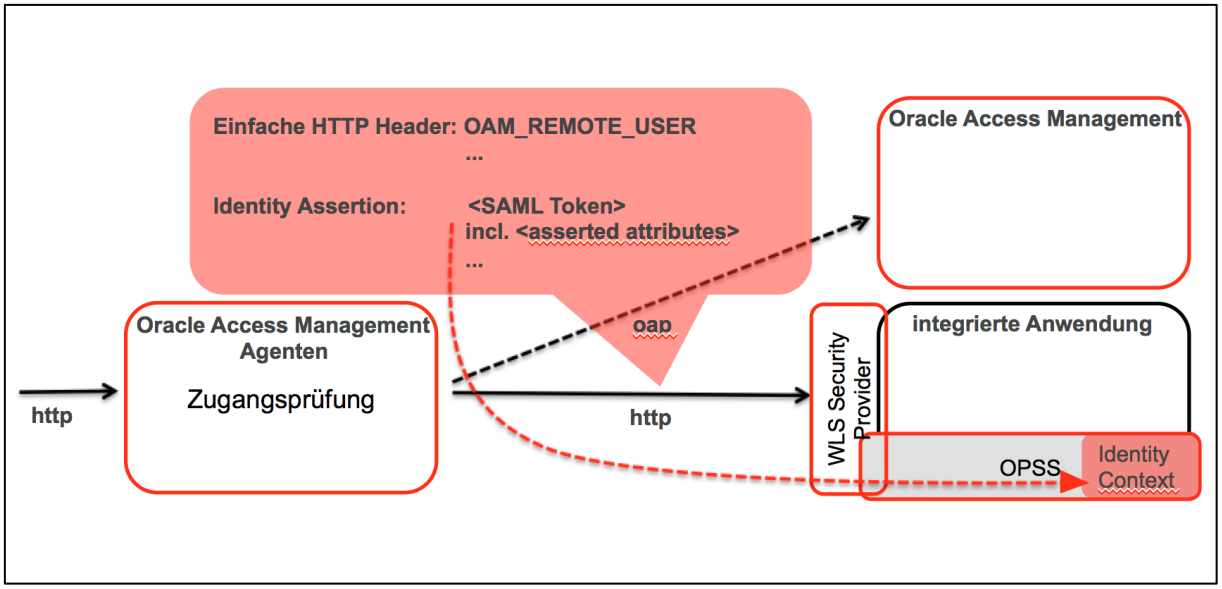

Abb. 3: Identity Propagation: die Identity Assertion

Die Security Provider des WLS der integrierten Anwendung überprüfen die Identity Assertion und schreiben die zugesicherten Attribute via OPSS in den Identity Context. Dort sind sie über das OPSS IDC-API für die Anwendung verfügbar und können auf mehreren Wegen für Autorisierungsentscheidungen herangezogen werden.

Beim Aufruf von abgesicherten Webservices durch die Anwendung wird der OWSM Agent so konfiguriert, dass er neben dem authentifizierten Nutzer auch die zusätzlichen Attribute aus dem Identity Context im SOAP Header mitschickt. Voraussetzung dafür ist eine OWSM-Policy, die ein SAML Token verwendet.

Der OWSM-Agent beim Webservice Producer wiederum wertet das SAML Token aus und schreibt die zusätzlichen Attribute in den Identity Context. Auch hier sind sie über das OPSS IDC-API für die Anwendung verfügbar und können für Autorisierungsentscheidungen herangezogen werden.

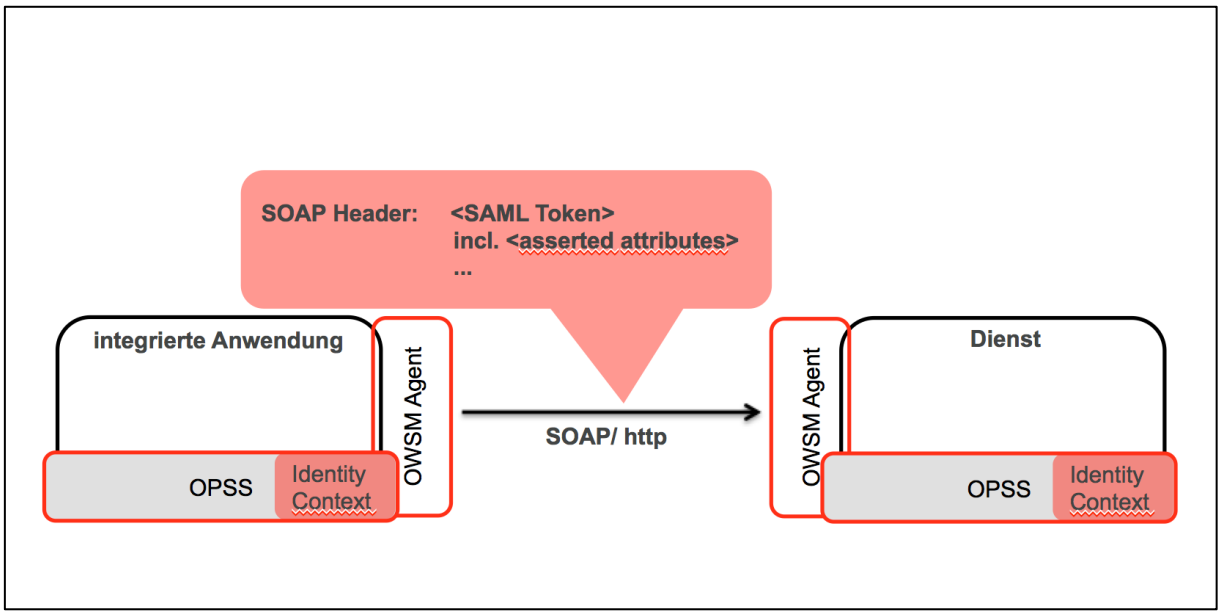

Abb. 4: Identity Propagation und Identity Context

Auf diesem Wege werden Nutzeridentität und Context vom Access Management über Agenten und abgesicherte Webservice-Aufrufe bis ins Backend übertragen und stehen integrierten Anwendungen und Diensten über ein- und dieselbe Schnittstelle zur Verfügung. Die Verteilung des Identity Contexts ist

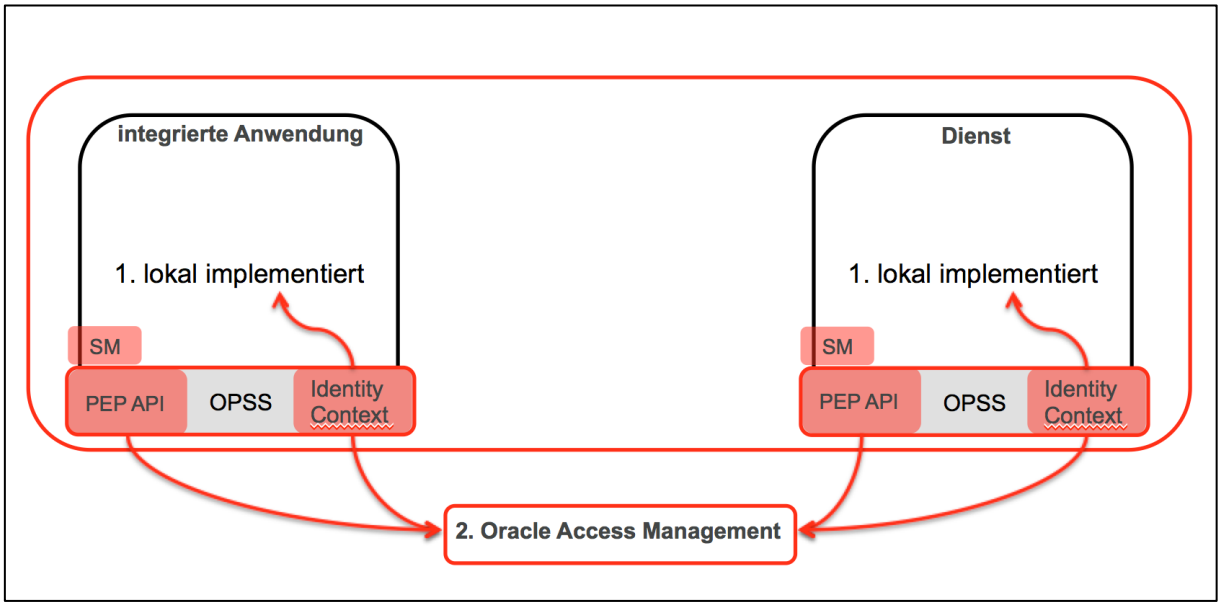

Abb. 4: Autorisierungs-Optionen mit Hilfe des Identity Contexts

Anwendungen oder Dienste haben nun mehrere Möglichkeiten, den Identity Context zur Autorisierung zu nutzen:

- bei lokal implementierter Autorisierung über das OPSS IDC-API
- über ein fertiges Security Modul des OES (Teil des Oracle Access Management) werden Autorisierungsentscheidungen an OES verlagert; die Policies des OES haben Zugriff auf den Identity Context
- letzterer Mechanismus kann auch über direkte Nutzung des OES PEP-APIs angesteuert werden

Die Autorisierungs-Entscheidungen auf Basis des Identity Context müssen nun nicht unbedingt immer zur Verweigerung eines Zugriffs führen, sondern können durchaus auch nur das Ergebnis beeinflussen, beispielsweise einen geringeren Datenumfang zurückliefern.

Kontaktadresse:
Klaus Scherbach
Oracle Deutschland B.V. & Co. KG
Hamborner Str. 51
D-40472 Düsseldorf

Telefon: +49 (0) 171 143 1661
E-Mail Klaus.Scherbach@oracle.com
Internet: www.oracle.com