IT-Sicherheit und Oracle Fusion Middleware: eine Herkulesaufgabe?

Mohammad Esad-Djou

Frank Burkhardt

OPITZ CONSULTING GmbH
München/Nürnberg

Schlüsselworte

IT-Security, Authentication, Authorization, Single Sign-on (SSO), Secure Socket Layer (SSL), WebLogic Server, PKI, Certificate, OAM, OID, OVD, WebGate.

Einleitung

Die Anforderungen, die heute an IT-Sicherheitsexperten gestellt werden, erinnern mitunter an die scheinbar unlösbaren Aufgaben des Herkules in der griechischen Sage. Doch nicht jeder Security-Spezialist ist ein IT-Muskelmann. Und allein die traditionellen IT-Sicherheitsansätze und Maßnahmen reichen nicht aus, um neue technische aber auch organisatorische Fragen zu beantworten. Welche Lösungsansätze bietet Oracle aus diesem Dilemma? Nach einer kurzen Einführung in die Problematik stellen die Referenten die Security-Konzepte von Oracle vor und richten danach einen besonderen Fokus auf Oracle WebLogic Server und Oracle Plattform Security Services (OPSS).

Diese Themen stehen dabei im Mittelpunkt:

- Herausforderungen der IT-Sicherheit in weltweit vernetzten Systemen
- IT-Sicherheitsarchitektur und der Ansatz von Oracle
- Oracle Fusion Middleware und Bausteine der Sicherheitstechnologie von Oracle: WLS, OAM, OID, OVD und WebGate
- Sichere Systeme: Best Practice und Erfahrungsberichte zu Authentication, Authorization, Single Sign-on (SSO), Secure Socket Layer (SSL) und Security Assertion Markup Language (SAML).

Herausforderungen

IT-Architekturen werden insbesondere im Middleware Bereich immer komplexer. Dies ist auch der Tatsache geschuldet, dass heterogen Systeme in ein Sicherheitskonzept integriert werden müssen. Eine sichere IT-Infrastruktur zu implementieren und zu pflegen ist in vielen Rechenzentren aus verschiedenen Gründen eine große Herausforderung. Die folgenden Aspekte sind dabei immer wieder vorzufinden.

Arbeitsteiligkeit

Für die Bereitstellung von IT-Infrastruktur sind häufig mehrere Abteilungen beteiligt, die sich in der Regel stringent arbeitsteilig organisieren. Klassisch ist z.B. eine strikte Trennung zwischen Betriebssystem und Middleware Software anzutreffen. Schnittstellen werden

dadurch häufig schlecht bis nicht besetzt, was zu erheblichen Verzögerungen führen kann. Sicherheitsaspekte bezüglich des eigenen Aufgabenbereichs werden berücksichtigt, nicht jedoch als ganzheitliches Ziel.

Security Gouvernance

Um ein ganzheitliches Sicherheitskonzept unternehmensweit zu realisieren und konstant halten zu können, wird eine unternehmensweite Institution mit einem ausreichenden Mandat benötigt. Diese Instanz erstellt Sicherheitskonzepte und Richtlinien und überwacht deren Einhaltung. In der Realität fehlt diese Einrichtung häufig ganz oder ist zu wenig präsent.

Technische Weiterentwicklungen

Themen wie Virtualisierung, Engineered Systems und Cloud Computing erhöhen die Komplexität für eine sichere IT-Infrastruktur. Middleware Cloud Systeme müssen in der Lage sein die geforderte Flexibilität, die an verteilte Echtzeitsysteme gestellt wird, zu gewährleisten. Verfügbarkeit als ein zentraler Sicherheitsaspekt kommt hier besonders zum Tragen. Cloud Computing als verteiltes Echtzeit-System: Die Kern-Herausforderung an solche Systeme ist eine Middleware Architektur, die in der Lage sein muss, die geforderte Flexibilität für die verteilten Echtzeit-Systeme gewährleisten zu können, aber auch die konkrete Antwort bzgl. Daten-Sicherheit im Cloud und Hochverfügbarkeit des Clouds geben zu können!

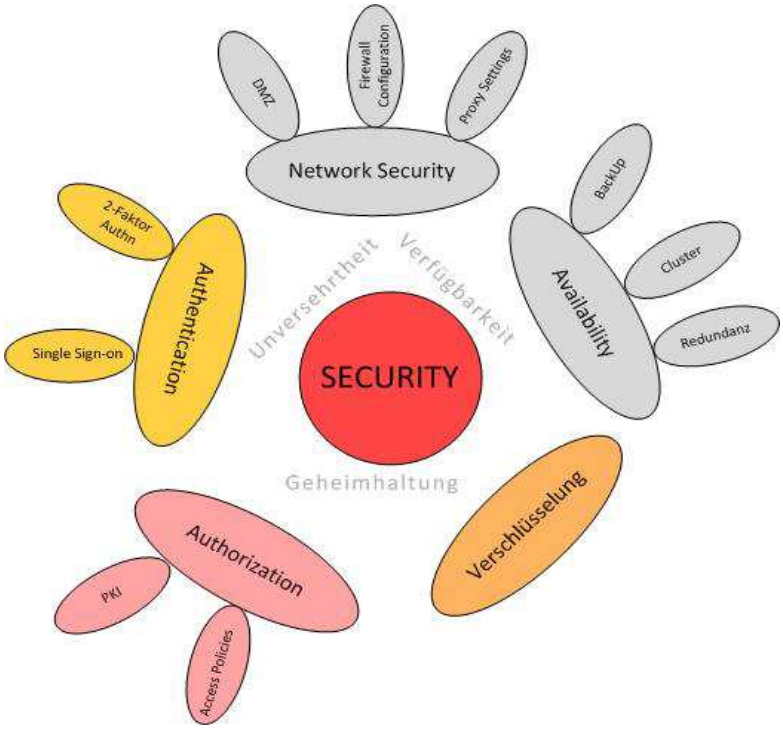

Abbildung 1 IT-Sicherheit: Herausforderungen

Was verstehen wir unter IT-Sicherheit?

Die drei Kernziele der IT Security sind Unversehrtheit, Geheimhaltung und Verfügbarkeit. Schnell wird klar, dass alleine mit diesem einfachen Ansatz die Komplexität sehr groß ist.

IT-Experten und Unternehmen müssen Antwort für ihre Sicherheitsfragen finden. Die grundlegenden Fragen zum Thema Sicherheit kommen einer Anforderungsanalyse gleich. Wie sich Anforderungen von Unternehmen an IT-Systeme erheblich unterscheiden, kann dies auch für den Sicherheitsbedarf deutlich der Fall sein. Ein grundsätzlicher Fragenkatalog gilt für alle. Ohne den Anspruch auf Vollständigkeit seien nur einige genannt:

- Existieren Vereinbarungen für den Umgang mit Daten und wie lauten diese?
- Welche Sicherheitsbedürfnisse und daraus resultierende Sicherheitsziele hat das Unternehmen?
- Wie sensibel sind meine Daten (personenbezogene Daten, Innovationen, etc.)?
- Was bedeutet die Nichtverfügbarkeit meiner Daten zu einer bestimmten Zeit?

Oracle Ansatz: Oracle Platform Security Services

OPSS ist eine Sicherheitsplattform für Java Applikationen, das eine umfassende Liste an Security Services bietet: Authentication, Autorisation, Credential Store Management, etc. Diese Dienste basieren auf Java-Technologien und haben einen einheitlichen Ansatz für Design und Anwendung von Sicherheitsrichtlinien auf Java EE und Ressourcen. OPSS als Enterprise Security Framework läuft auf dem WebLogic Server. Der OPSS-Authentifizierungsprozess ist in WebLogic Security integriert.

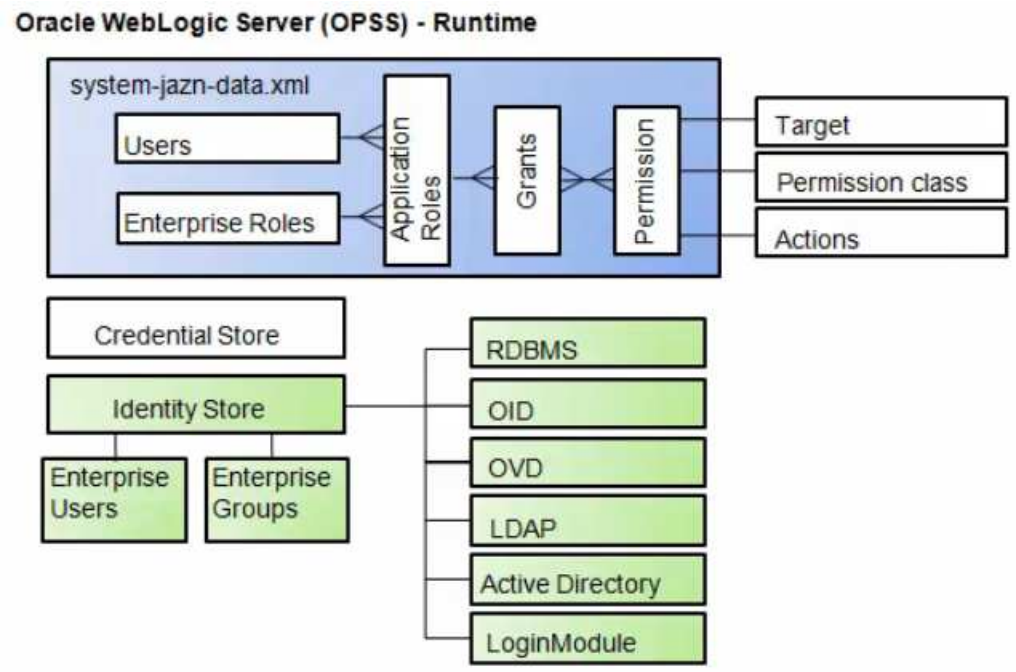

Abbildung 2 OPSS in WebLogic Server Runtime-Zustand

Abbildung 2 OPSS in WebLogic Server Runtime-Zustand zeigt, wie in WebLogic Server durch den Einsatz mehrerer Komponenten die Sicherheit von Ressourcen gewährleistet ist und kombiniert Sicherheits-Features von BEA (WebLogic Server, Oracle Entitlement Server (OES)) und Oracle Application Server 10g (OAS), wie z.B. Java Platform Security (JPS), vorherige JAZN. Damit können Anwendungsentwickler, System-Integratoren, Sicherheitsadministratoren und JEE-Anwendungen eine einheitliche Enterprise-Wide Sicherheitsplattform nutzen und eine unerwünschte Sicherheitsheterogenität vermeiden.

Weitere Vorteil von OPSS liegt darin, dass der gesamte OFM-Stack wie Oracle SOA, Oracle WebCenter, Oracle Application Development Framework (ADF), Oracle Forms, Reports usw. in die gemeinsame Sicherheitsplattform integriert werden kann. Wir werden in unserem Vortrag schrittweise einige wichtige Sicherheitsherausforderungen und Anwendungsfälle beschreiben und über Best Practice diskutieren.

Sichere Kommunikation: SSL, PKI…

Viele Firmen sind insbesondere daran interessiert, wie man in einer hochverfügbaren Umgebung mit vorgeschaltetem Hardware-LB die SSL-Konfiguration richtig aufsetzt. Es werden `Private Keys`, `Digital Certificates` und `Trusted Certificate Authorities` verwendet, um die Identität von Benutzern und/oder Servern zu überprüfen und Vertrauen zu etablieren. Wenn wir über sichere Kommunikationen diskutieren, dann müssen wir auf die folgenden Fragen Antworten bekommen: Ist der Browser für Single Sign-On (SSO) konfiguriert? Ist `Custom Identity Keystore` und `Custom Trust Keystore` konfiguriert? Wurde SSL Listen Port konfiguriert? Auf welchen Ports?

SSL

Im Allgemein bietet SSL den folgenden Möglichkeiten:

- Ein Mechanismus, dass die kommunizierenden Applikationen sich gegenseitig identifizieren und authentifizieren können.
- Verschlüsselung der ausgetauschten Daten von Anwendungen

In SSL-Kommunikation wird das Ziel (der Server) sich immer gegenüber dem Initiator (der Client) authentifiziert. Optional, wenn das Ziel (der Server) dies anfordert, kann der Initiator (der Client) sich auch dem gegenüber des Ziels authentifizieren. Die Datenübertragung wird verschlüsselt. Eine SSL-Verbindung beginnt mit einem Handshaking, in dem die Anwendungen digitale Zertifikate austauschen, sich auf die Verschlüsselungsalgorithmen einigen und die Verschlüsselungsschlüssel (encryption keys) generieren. Der Schlüssel wird für den Rest der Sitzung verwendet werden.

Wenn wir mehr Sicherheit in unserer IT-Landschaft brauchen, dann richten wir SSL in den Umgebungen ein. Mit anderen Worten konfigurieren wir die HTTPS-Protokolle und dazugehörige Elemente, wie etwa die Erstellung der Zertifikate, Anwenden von Private und Public Keys und Konfiguration des Keystores.

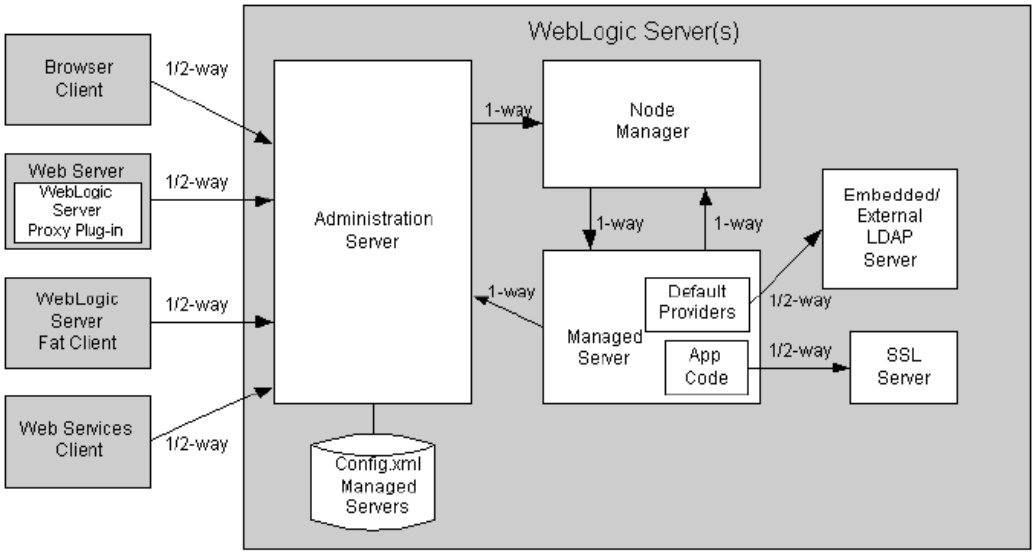

Abbildung 3 WebLogic Server: One-Way und Two-Way SSL Authentifizierung

Zertifikate

Die erste Frage lautet: Welche Zertifikate müssen wir erstellen? Die Erstellung drei verschiedener Zertifikaten ist möglich: `Self-Signed Certificate`, `Root CA Certificate` und `Intermediate CA Certificate`. Um vorhandene Zertifikaten auf z.B. MS Windows anzuschauen bzw. zu verwalten, können wir den Befehl `certmgr.msc` nutzen: Öffnen Sie die Zertifikatverwaltung, indem Sie auf die Schaltfläche Start klicken, `certmgr.msc` in das Feld Suche eingeben und dann die EINGABETASTE drücken. Wenn Sie aufgefordert werden, ein Administratorkennwort oder eine Bestätigung einzugeben, geben Sie das Kennwort bzw. die Bestätigung ein.

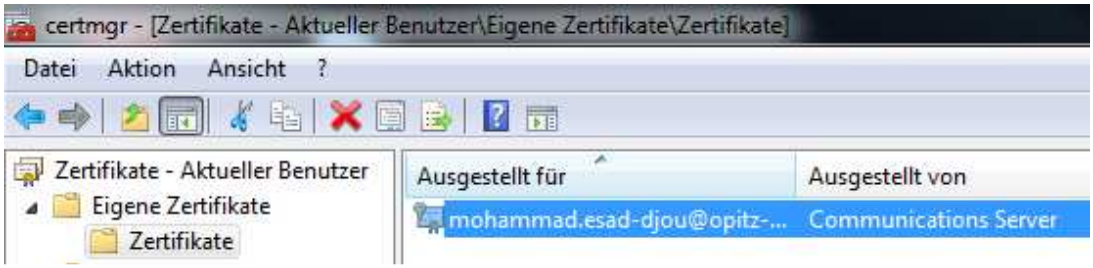

Abbildung 4 Eigene Zertifikate auf MS Windows

Self-Signed Certificate

`Self-Signed Certificates` sind Zertifikate, deren Felder „`Issued To`“ und „`Issued By`“ von der Entity selber ausgestellt wurden. Anders gesagt bestätigen sich diese Zertifikate selbst und deshalb nennt man sie: `Self-Signed Certificate`

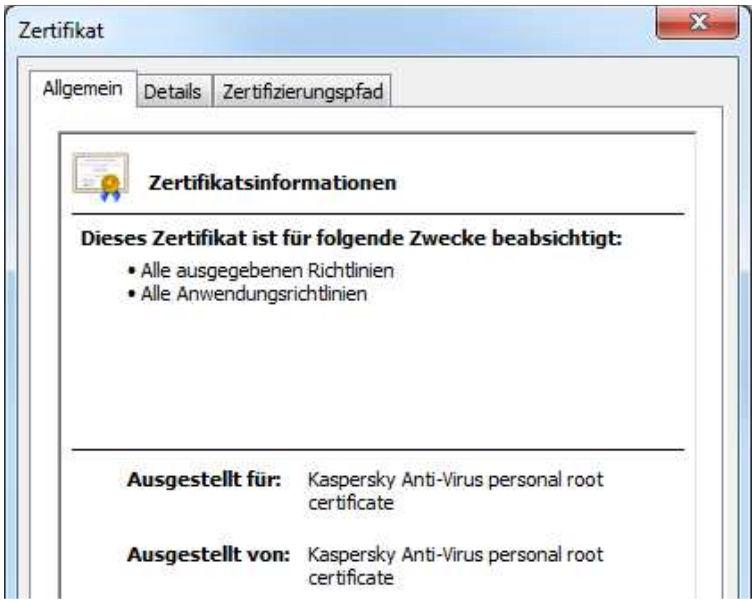

Abbildung 5 Beispiel eines Self-Signed Certificate

Root CA Certificate

`Root CA Certificate` ist ein **CA** Zertifikate, das einfach ein `Self-signed Certificate` ist. Das Zertifikat repräsentiert eine Entität, die das Zertifikat ausgestellt hat und ist als `Certificate Authority (CA)` bekannt. Die Anwendung dieser Zertifikate unterscheidet sich von anderen normalen Zertifikaten.

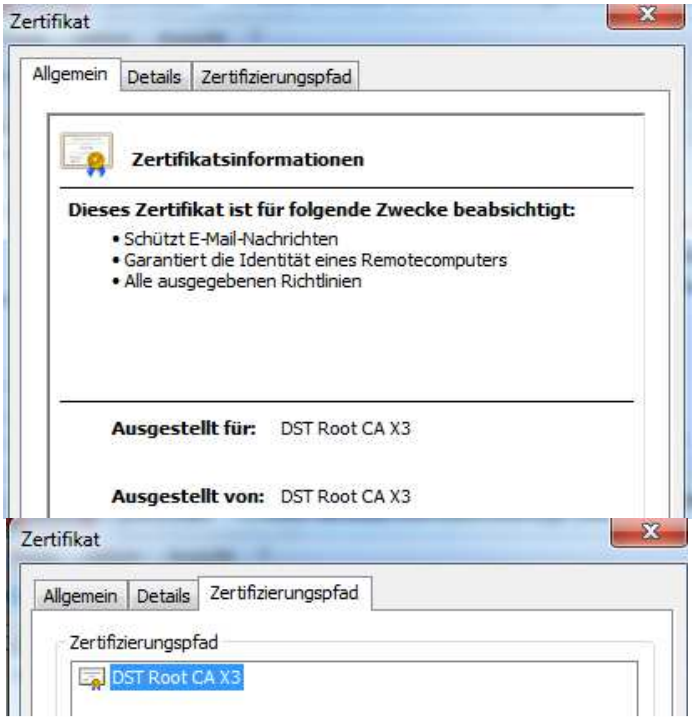

Abbildung 6 Beispiel eines Root CA

Intermediate CA Certificate

`Intermediate CA` Zertifikat ist ein CA Zertifikat, das kein `Self-signed Certificate` ist. Dieses Zertifikat kann ein Root CA sein.

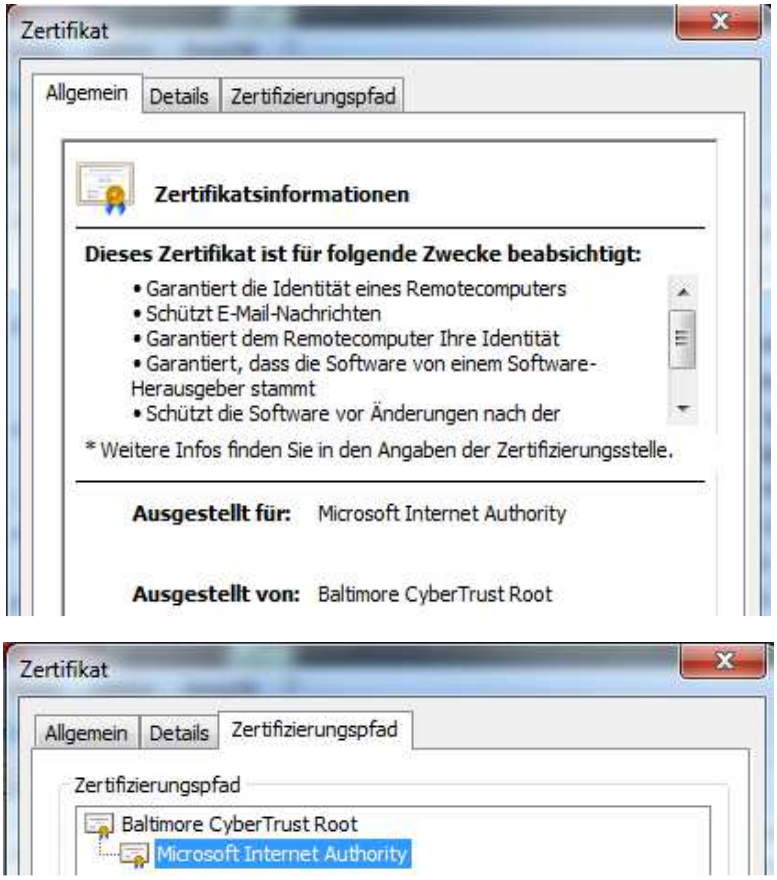

Abbildung 7 Beispiel eines Intermediate CA

PKI

Ein weiteres Element für die Ausrichtung sicherer IT-Kommunikation ist die Erstellung und Verwendung von Public und Private Keys. Der öffentliche Schlüssel (`Public Key`) ist in ein digitales Zertifikat eingebettet. Ein privater Schlüssel und digitales Zertifikat ermöglichen es, die Identität festzulegen.

Die vertrauenswürdige Zertifizierungsstelle (`Certificate Authority - CA`) schafft Vertrauen für ein Zertifikat. Zertifikate und Zertifikatsketten müssen geprüft werden, bevor eine Vertrauensbeziehung aufgebaut werden kann. Um die Zertifikate zu generieren, müssen wir das Keytool verwenden. Keytool, als eine Datenbank von Schlüsseln, ist ein Standard-Java-Utility.

WLS: Identity und Trust

WebLogic Server unterstützt SSL-Kommunikation, die die sichere Kommunikation zwischen über das Web verbundenen Applikationen ermöglicht. WebLogic Server liefert ein Pure-Java Implementation von SSL. WebLogic Server (WLS) ist als Default mit `Demo`

`Identity` und `Demo Trust` konfiguriert. Wir brauchen nur den SSL-Port zu aktivieren. Jedoch ist die Anwendung von `Demo Identity` und `Demo Trust` in Live-Systemen nicht zu empfehlen ist. Im Vortrag wird die Erstellung von Identity und Trust Keystores präsentiert[1].

Authentication: Wer bist du?

Typische Fragen, die die IT-Sicherheit bezüglich der Authentifizierung beantworten sollte, sind: Welche Authentifizierungsverfahren sind vorhanden? Und welche sind geplant? Hardware-Token, Passwort, Chipkarte/Smartcard, biometrische Verfahren, SSL-Zertifikate?

Authentifizierung überprüft die tatsächliche Identität von Benutzern. Der Benutzer kann auch ein Entität oder eine Person, eine Software oder andere Instanzen sein. In WebLogic Server wird „Benutzer" als „Ressourcen" ausgedrückt. WLS führt Beweis-Material (`proof material`) in der Regel durch ein JAAS LoginModule. JAAS-Authentifizierung ist in einem Pluggable-Verfahren implementiert. Die Identität eines Benutzers wird durch die Anmeldeinformationen dieses Benutzers bestätigt, z.B.:

1- ein physikalisches Objekt, z.B. Anmeldeinformationen, die von einer vertrauenswürdigen Stelle ausgestellt wurde, wie ein Reisepass oder eine Chipkarte
2- eine geheime Information, z.B. ein Passwort oder eine PIN
3- eine einzigartige personenbezogene Information, z.B. biometrische Informationen wie ein Fingerabdruck oder Irismuster

Eine Kombination mehrerer Arten von Anmeldeinformationen wird als "starke" Authentifizierung bezeichnet; z.B. mit einem ATM-Karte (Credential 1) mit einer PIN oder Passwort (Credential 2).[2]

Arten von Authentifizierung

WebLogic Server ist in der Lage, die verschiedenen Arten der Authentifizierung durchzuführen, weil es die WebLogic Authentifizierungsanbieter oder benutzerdefinierte Sicherheitsanbieter (`Authentication provider` or `custom security providers`) verwenden kann. Im Vortrag werden unterschiedliche Authentifizierungstypen, wie z.B. Basic Authentication, Certificate Authentication, Digest Authentication und Perimeter authentication (darunter SAML-Verfahren) diskutiert.

Directory Service: OID und OVD

Basis für die Authentifizierung ist ein Identity Store. Meist werden die Benutzer eines Unternehmens zentral in einem Microsoft Active Directory (AD) verwaltet. Oracle bietet in seinem Produktportfolio Thema Identity Management (IDM) gleich mehrere Directory Services (Identity Stores), sowie Oracle Unified Directory (OUD), Oracle Internet Directory (OID) und Oracle Virtual Directory (OVD) an.

Oracle Internet Directory ist ein universeller Verzeichnisdienst, der den schnellen Abruf und zentrale Verwaltung von Informationen über verteilte Benutzer und Netzwerkressourcen ermöglicht. Es verbindet das Lightweight Directory Access Protocol (LDAP) Version 3 mit der hohen Leistung, Skalierbarkeit, Robustheit und Verfügbarkeit einer Oracle-Datenbank[3].

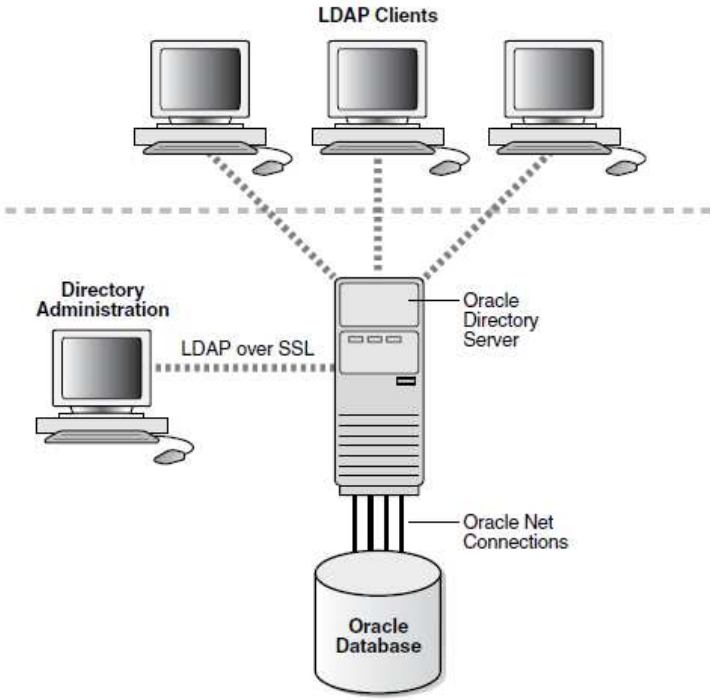

Abbildung 8 Oracle Internet Directory: Überblick

Das OVD ist ein LDAP v3 Service, der als Fassade zum Zugriff auf einen oder mehrere Enterprise Directory Server und Datenbanken dient. Dieser Dienst wird benötigt, wenn mehrere Directory Server integriert werden sollen und wenn es sich um Benutzerdaten handelt, die in Datenbanken vorgehalten werden. Es wird benötigt, um die OID-Datenbank für OAM nutzen zu können, da OAM für Benutzerdaten ein LDAP-Interface voraussetzt. Im Falle eines Datenbank Stores realisiert das OVD ein Mapping von Attributen auf LDAP-Attribute.

Autorisierung: Access Control

Autorisierung ist auch als Zugangskontrolle bekannt und wird verwendet, um Hauptfragen zu klären, wie: „Worauf können Sie zugreifen?“, „Wer hat Zugang zu einem WebLogic Ressource?“, „Ist der Zugriff erlaubt?“ und in der Regel „Wer kann was tun?“. Um die Integrität, Vertraulichkeit (Schutz der Privatsphäre) und die Verfügbarkeit von Ressourcen zu gewährleisten, schränkt WebLogic den Zugriff auf seine Ressourcen ein.

SSO

Single-Sign-On (SSO) ermöglicht es, dass ein Benutzer nach einer Authentifizierung an einem Arbeitsplatz auf alle Systeme und Anwendungen, für die er lokal berechtigt ist, zugreifen kann, ohne sich neu anmelden zu müssen. Eine SSO-Lösung von Oracle basiert auf dem Einsatz von OAM. Damit werden weitere Komponenten, die in den vorherigen Abschnitten vorgestellt haben, in eine Gesamtlösung integriert.

Oracle Access Manager (OAM) und Access Server

Die OAM Access Server bieten die wesentlichen Dienste des OAM an. Dazu zählen Authentifizierung, Autorisierung und Single-Sign-On. Skalierung und Hochverfügbarkeit

werden u.a. durch die Einrichtung weiterer Access Server und eine entsprechende Konfiguration der Webgates erreicht. OAM schreibt Session-Daten, AuditLogs sowie Konfigurationsinformationen (Policies) in Datenbanktabellen (JDBC). Die Verteilung von Session-Daten über OAM-Instanzen hinweg erfolgt mittels einer InMemory Datenbank (Oracle Coherence). Der OAM Access Server ist zentraler Policy Decision Point (PDP) und bietet Dienste wie Authentifizierung, Autorisierung und Single Sign-On an, aber auch Policy Management und Auditing an. Der OAM ist eine Weblogic Server basierte Anwendung.

Webtier: Apache, OHS, WebGate

Der Webserver auf Apache Basis bzw. OHS tritt als Reverse Proxy vor den Applikationen auf. Er beinhaltet darüber hinaus ein OAM Webgate. Das WebGate ist ein Security Gateway für die Integration in einen Webserver. Es dient als Policy Enforcement Point (PEP) und setzt die vom OAM Server (PDP) für bestimmte URLs (sogenannte „geschützte URLs) vorgegebenen Policies betreff Authentifizierung und Autorisierung durch. Darüber hinaus ist das Webgate in der Lage, in den OAM Policies definierte Aktionen auf HTTP(S)-Requests durchzuführen. So kann es z.B. Cookies setzen, HTTP(S)-Header oder die OAM Session mit Anwenderdaten befüllen und diese den integrierten Anwendungen so zugänglich machen.

- Wir werden ein klassische SSO-Szenarios, dass OAM, OVD, OID, WebGate und OHS von Oracle-Welt mit Windows Active Directory integriert, im Vortrag vorstellen.

Kontaktadresse:
Frank Burkhardt
OPITZ CONSULTING GmbH
Zeltnerstraße 3
D-90443 Nürnberg

Telefon: +49 (89) 680098-0
Fax: +49 (89) 680098-4400
E-Mail Frank.Burkhardt@opitz-consulting.com
Internet: http://www.opitz-consulting.com

Mohammad Esad-Djou
OPITZ CONSULTING GmbH
Weltenburger Straße 4
D-81677 München

Telefon: +49 (89) 680098-0
Fax: +49 (89) 680098-4400
E-Mail Mohammad.Esad-Djou@opitz-consulting.com
Internet: http://www.opitz-consulting.com
http://modj.org/
http://thecattlecrew.wordpress.com/

[1] Also refer Note 1218695.1 for configuring SSL in FMW 11G: http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html und

http://docs.oracle.com/cd/E11035_01/wls100/secmanage/identity_trust.html

[2] See Oracle Fusion Middleware Security Overview http://docs.oracle.com/cd/E23943_01/core.1111/e12889.pdf
Oracle Fusion Middleware 11.1.1.5, Security Guides http://docs.oracle.com/cd/E21764_01/security.htm
Oracle® Fusion Middleware Securing Oracle WebLogic Server http://docs.oracle.com/cd/E21764_01/web.1111/e13707/toc.htm
Oracle Platform Security Services 11gR1 (White Paper) http://www.oracle.com/technetwork/middleware/id-mgmt/opss-tech-wp-131775.pdf

[3] Oracle® Fusion Middleware: Administrator's Guide for Oracle Internet Directory, 11g Release 1 (11.1.1), E10029-06