OPITZ CONSULTING

Menschen. Innovationen. Lösungen.

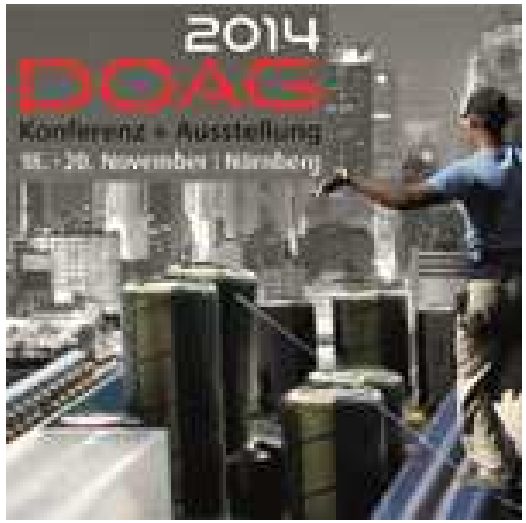
IT-Sicherheit und OFM:

Eine Herkulesaufgabe?

Mohammad Esad-Djou, Solution Architect

Frank Burkhardt, Senior Consultant

OPITZ CONSULTING Deutschland GmbH



Nürnberg, 20.11.2014

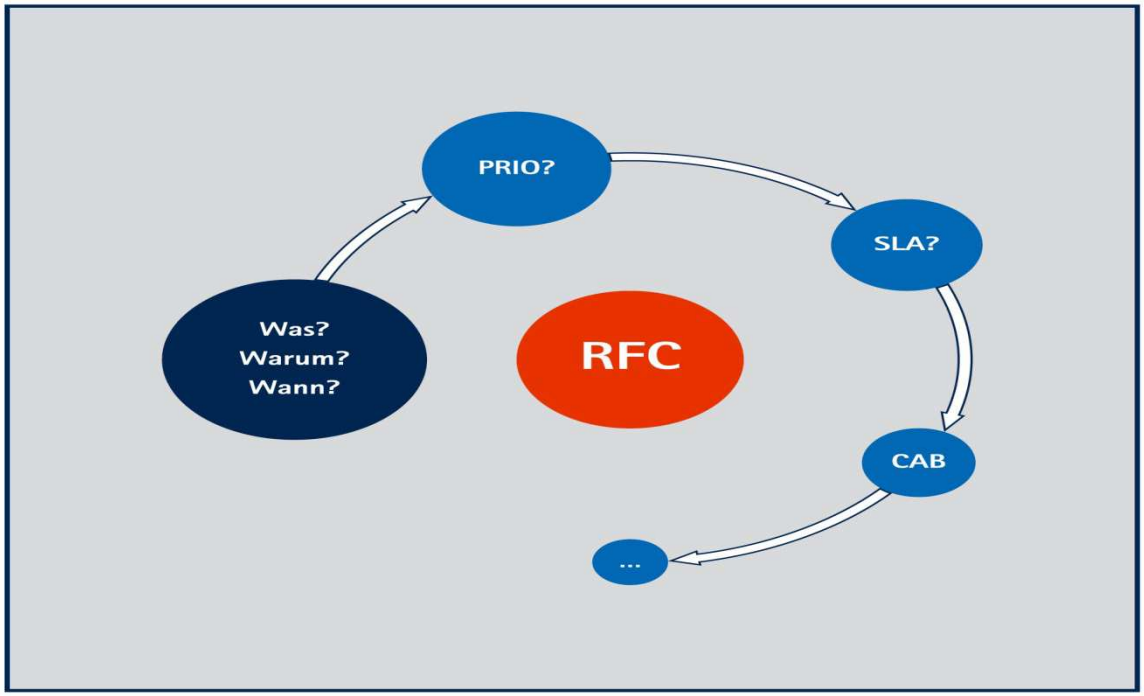
Agenda

1. Herausforderungen
2. Was verstehen wir unter IT-Sicherheit?
3. Oracle Ansatz: Konzept und Komponente
4. Sichere Kommunikation: SSL, PKI…
5. Forms Single-Sign-on Integration State of the Art
6. Zusammenfassung

Security im Alltag!

Darf man eigentlich nach Telefonaten fremder Leute in der Bahn Fragen stellen, wenn einem etwas unklar geblieben ist?

Organisation komplexer IT Infrastruktur



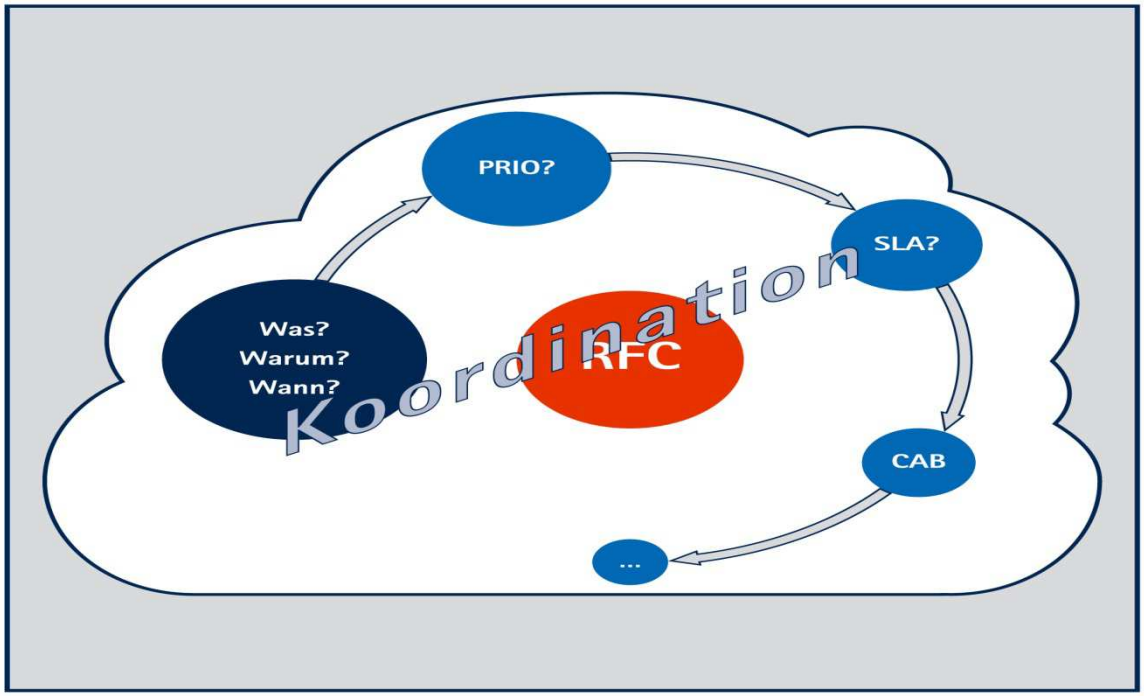
Network Management

Middleware Management

Database Management

OS Management

Organisation komplexer IT Infrastruktur



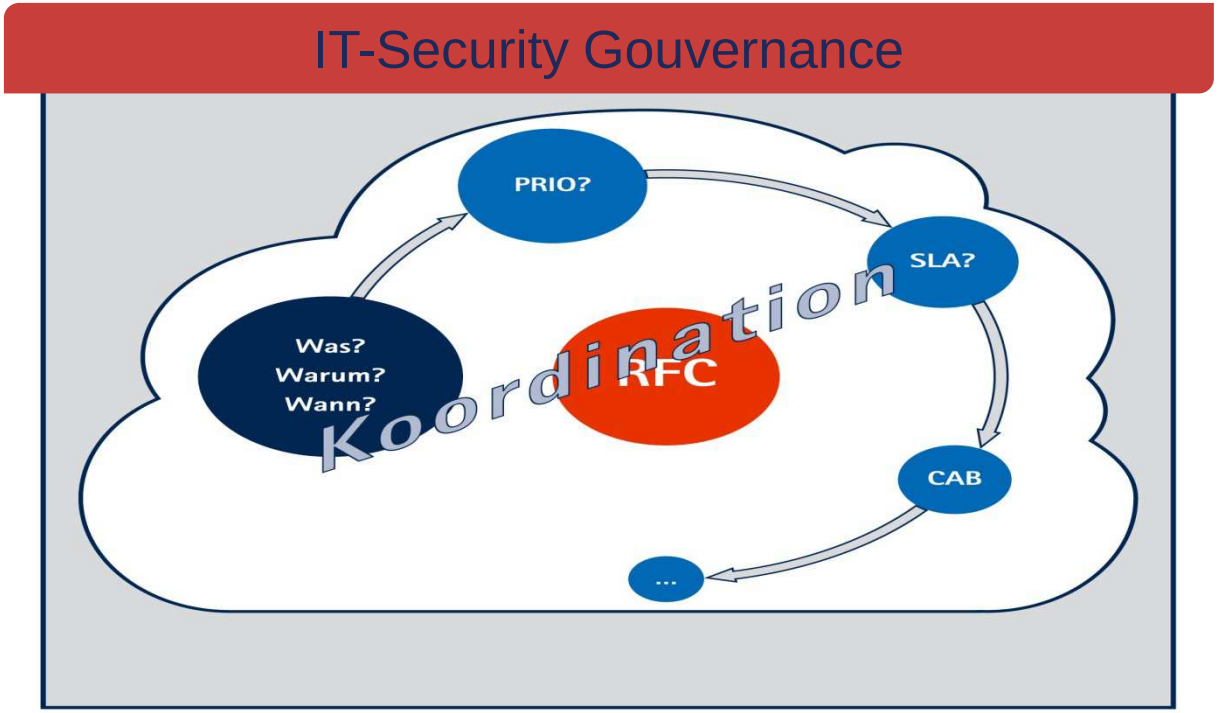
Network Management

Middleware Management

Database Management

OS Management

IT-Security und IT-Prozesse



Network Management

Middleware Management

Database Management

OS Management

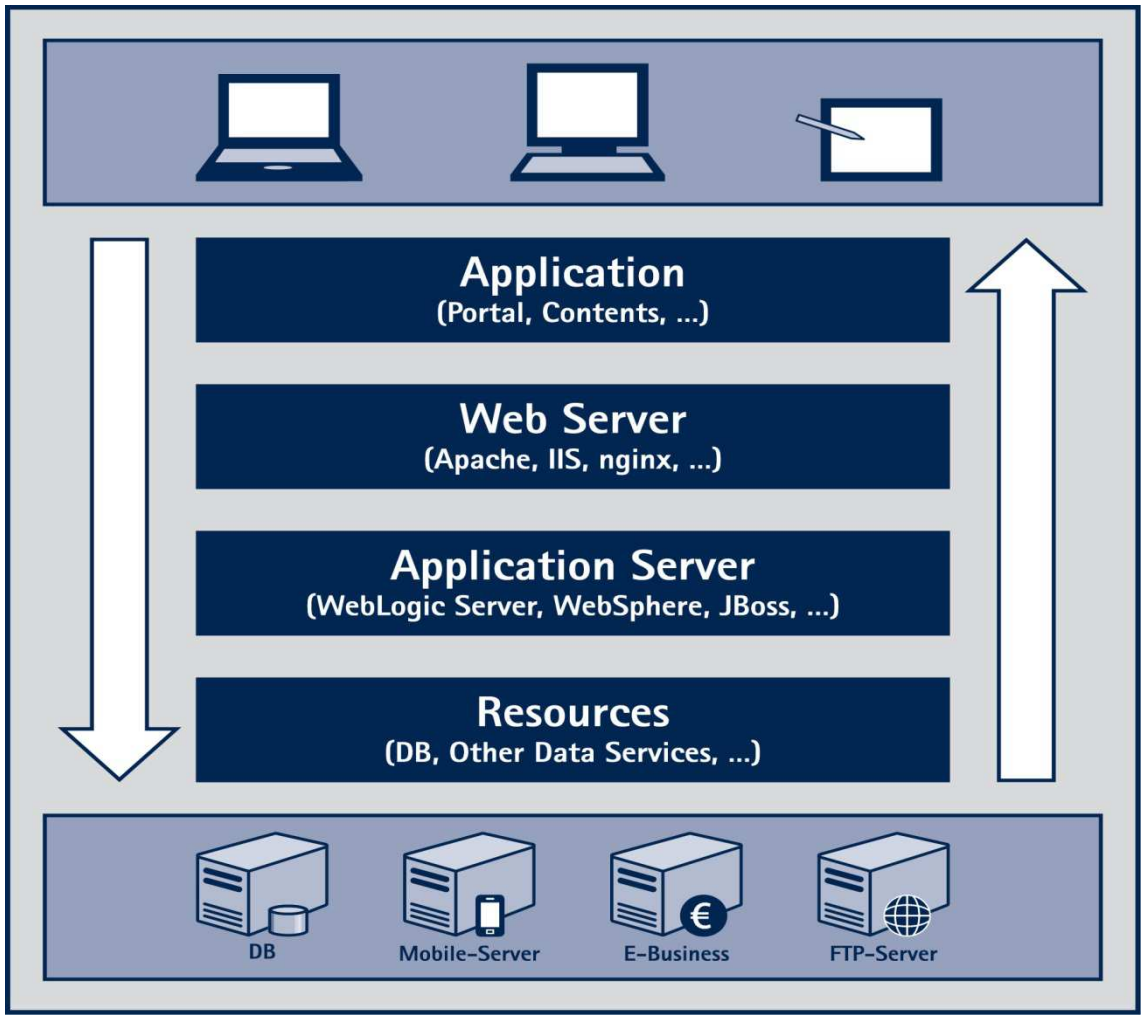
Wann ist Security-Relevanz gegeben?

- Auswirkungen auf den Betrieb einer Perimeter Firewall
- Auswirkungen auf den Betrieb einer internen Firewall
- Auswirkungen auf eine Komponente zur Berechtigungsprüfung
- Auswirkungen auf die Passwort-Policy
- Änderung von Logging-Einstellungen
- Veränderungen an Kommunikationsbeziehungen oder Netzebenen
- Auswirkungen auf die Sicherheit des Gesamtkonzepts
- …

Agenda

1. Herausforderungen
2. Was verstehen wir unter IT-Sicherheit?
3. Oracle Ansatz: Konzept und Komponente
4. Sichere Kommunikation: SSL, PKI…
5. Forms Single-Sign-on Integration State of the Art
6. Zusammenfassung

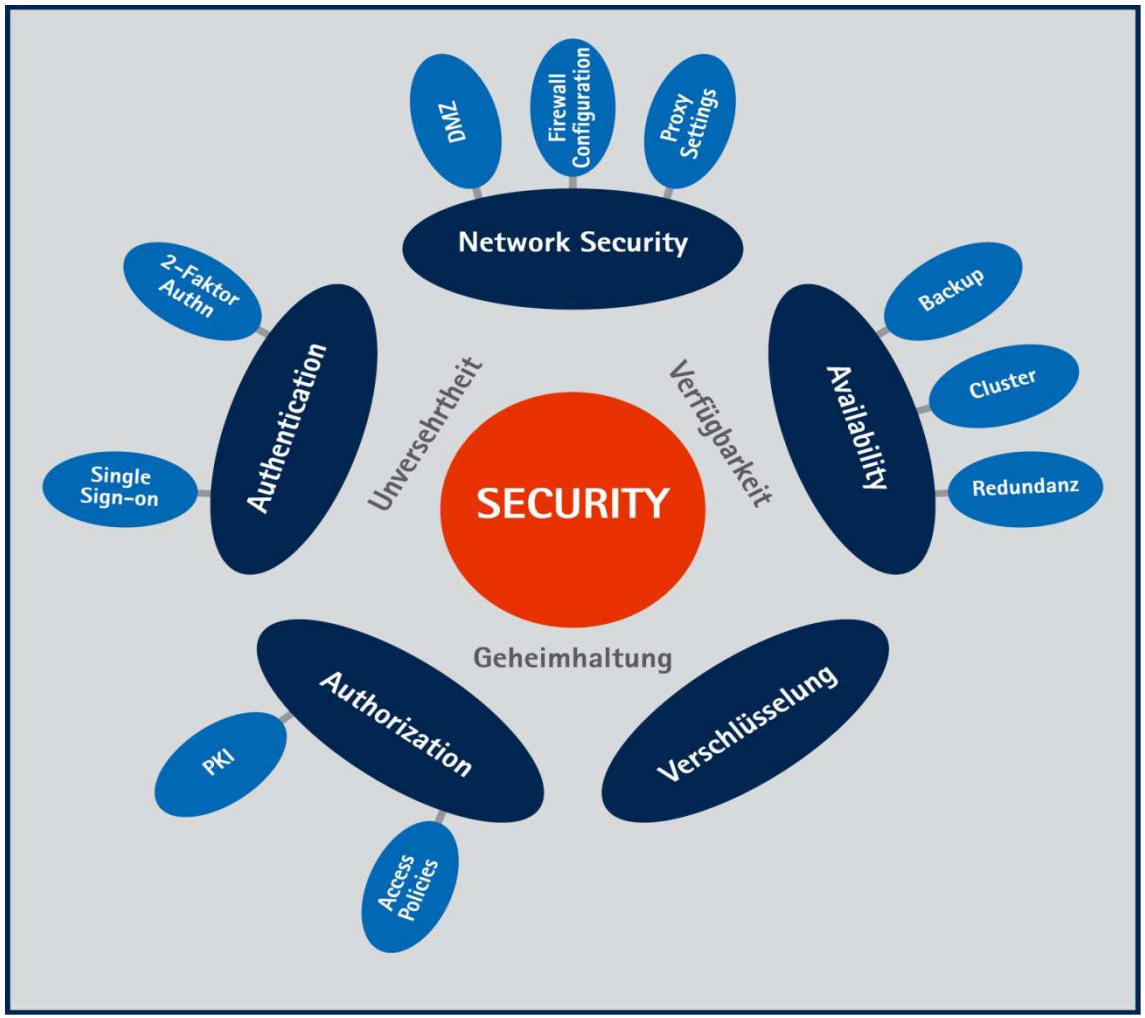
Security Challenges



Was verstehen wir unter IT-Sicherheit?

- **Kernziele der IT-Security: Unversehrtheit, Geheimhaltung und Verfügbarkeit**
- **Welche Sicherheitsbedürfnisse und daraus resultierende Sicherheitsziele hat das Unternehmen?**
- **Was bedeutet die Nichtverfügbarkeit meiner Daten zu einer bestimmten Zeit?**
- **Existieren Vereinbarungen für den Umgang mit Daten?**

Was verstehen wir unter IT-Sicherheit?



IT-Sicherheit

- **Verfahren zur Gewährleistung, dass die in einem Computer gespeicherten oder zwischen Computern übergebenen Daten nicht gefährdet sind**
- **Sicherheitsmaßnahmen**
  - **Proof material**
  - **Datenverschlüsselung**
- **Authentication, Authorization und Verschlüsselungsdienste**

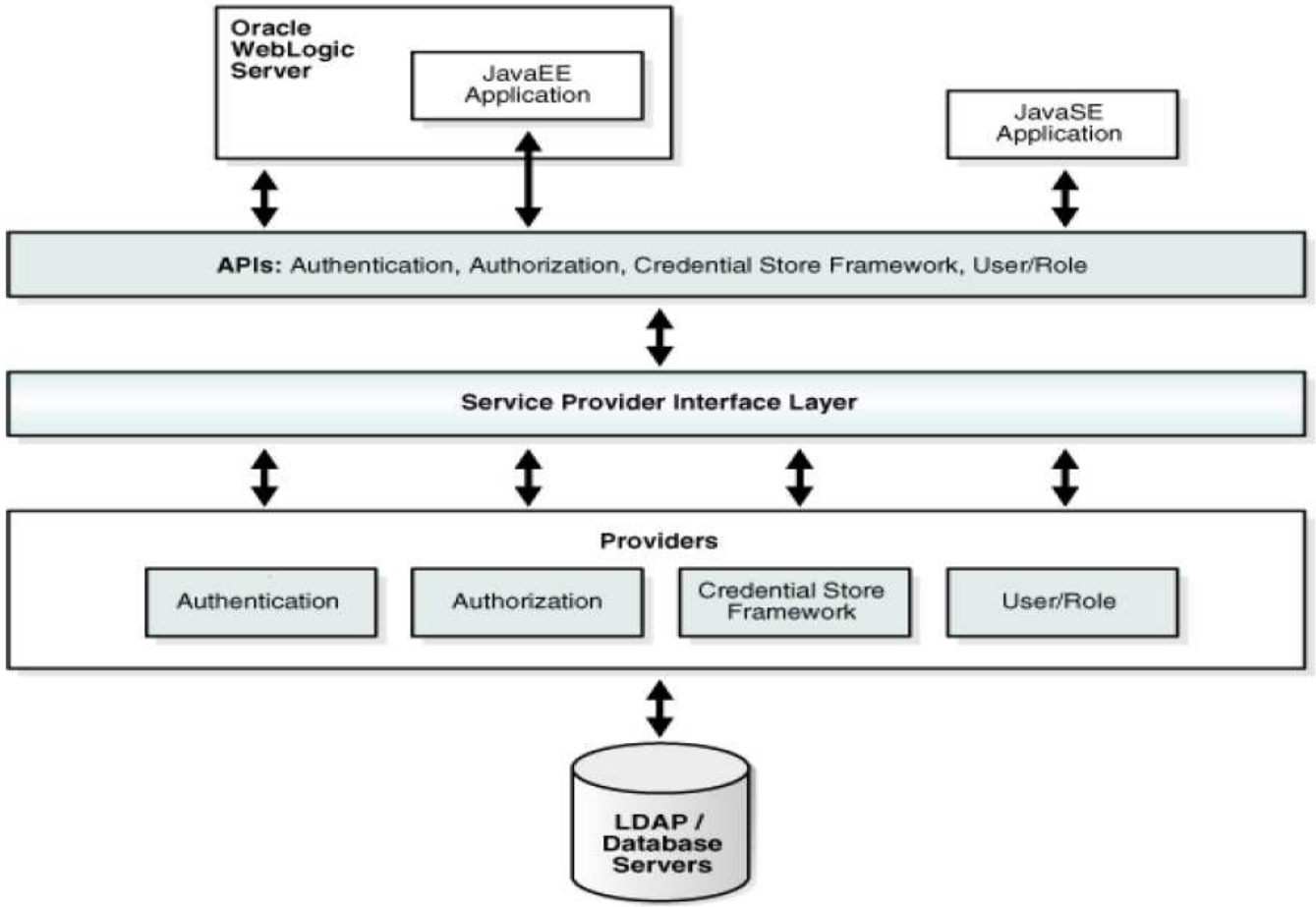
Agenda

1. Herausforderungen
2. Was verstehen wir unter IT-Sicherheit?
3. Oracle Ansatz: Konzept und Komponente
4. Sichere Kommunikation: SSL, PKI…
5. Forms Single-Sign-on Integration State of the Art
6. Zusammenfassung

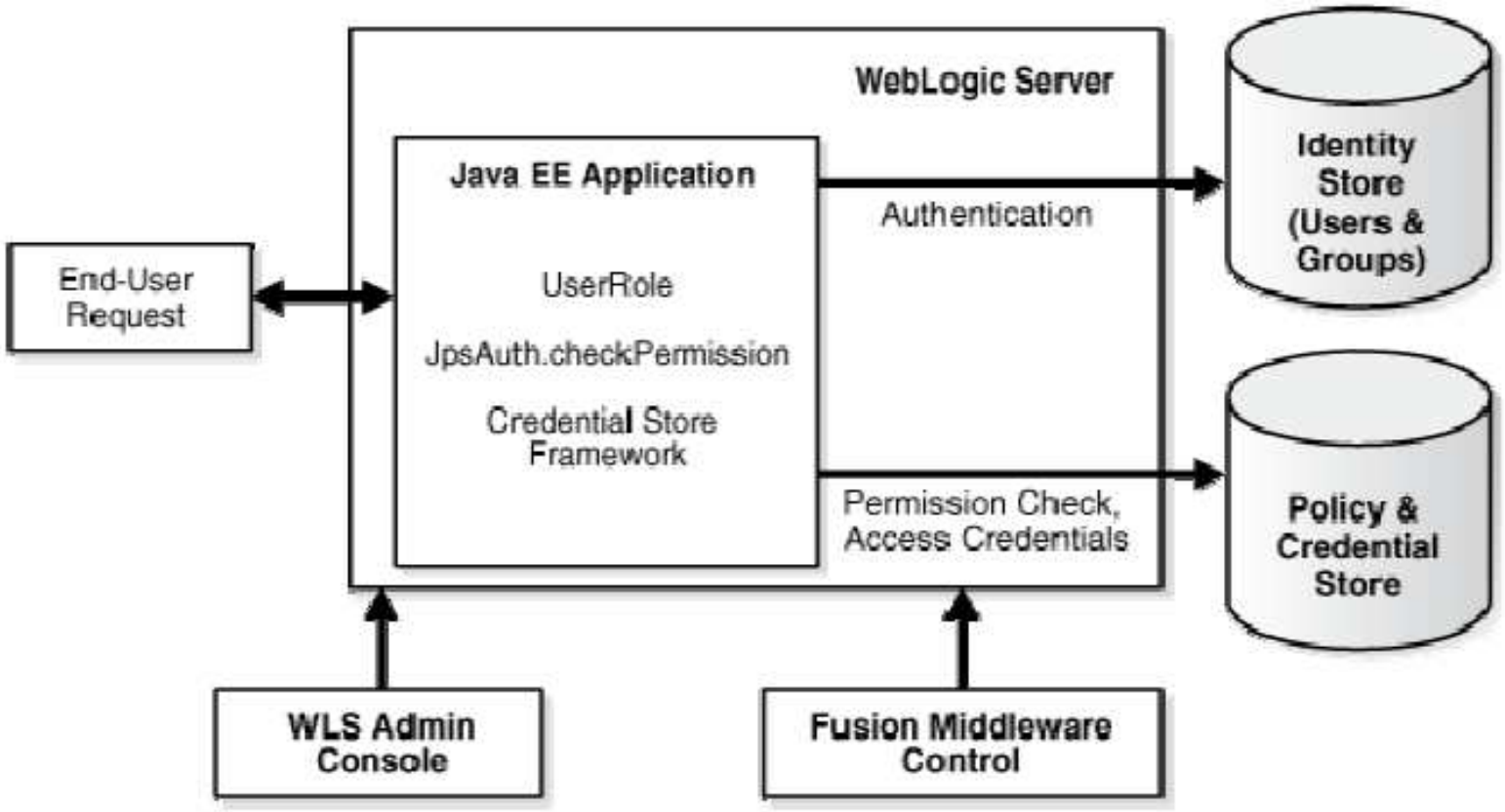
Oracle Platform Security Services

- **Einen Rahmen, der eine umfassende Reihe von Sicherheitsdienstleistungen bietet**
- **Java SE Fähigkeiten: Security APIs**
- **Java EE bietet zusätzliche Sicherheitsfunktionen**
- **Java Mangel**
  - **Audit**
  - **Single-Sign-on**
  - **Fine-Grained Authorization**
  - **Management Tooling**

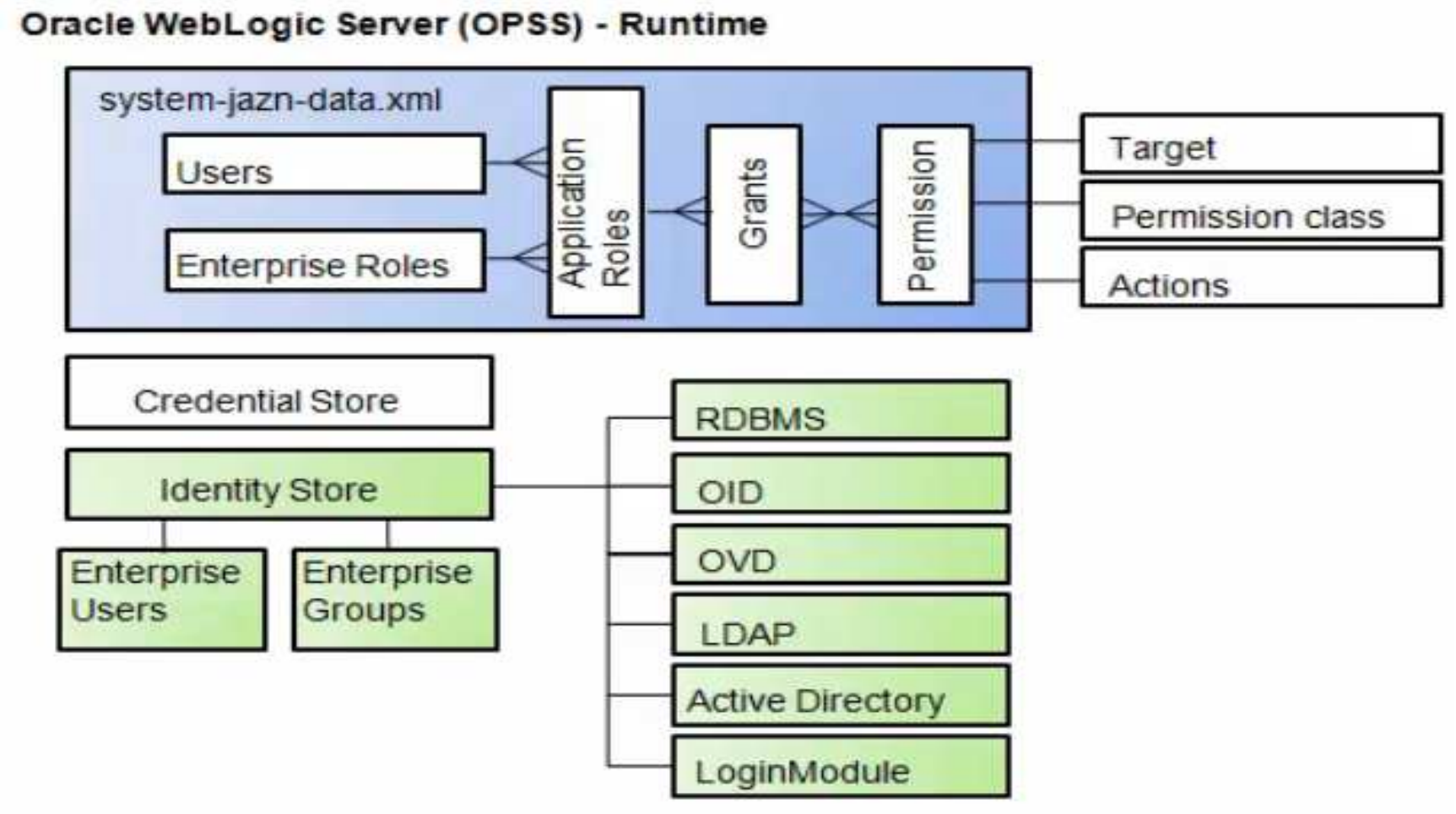
OPSS:
Architecture - Application View



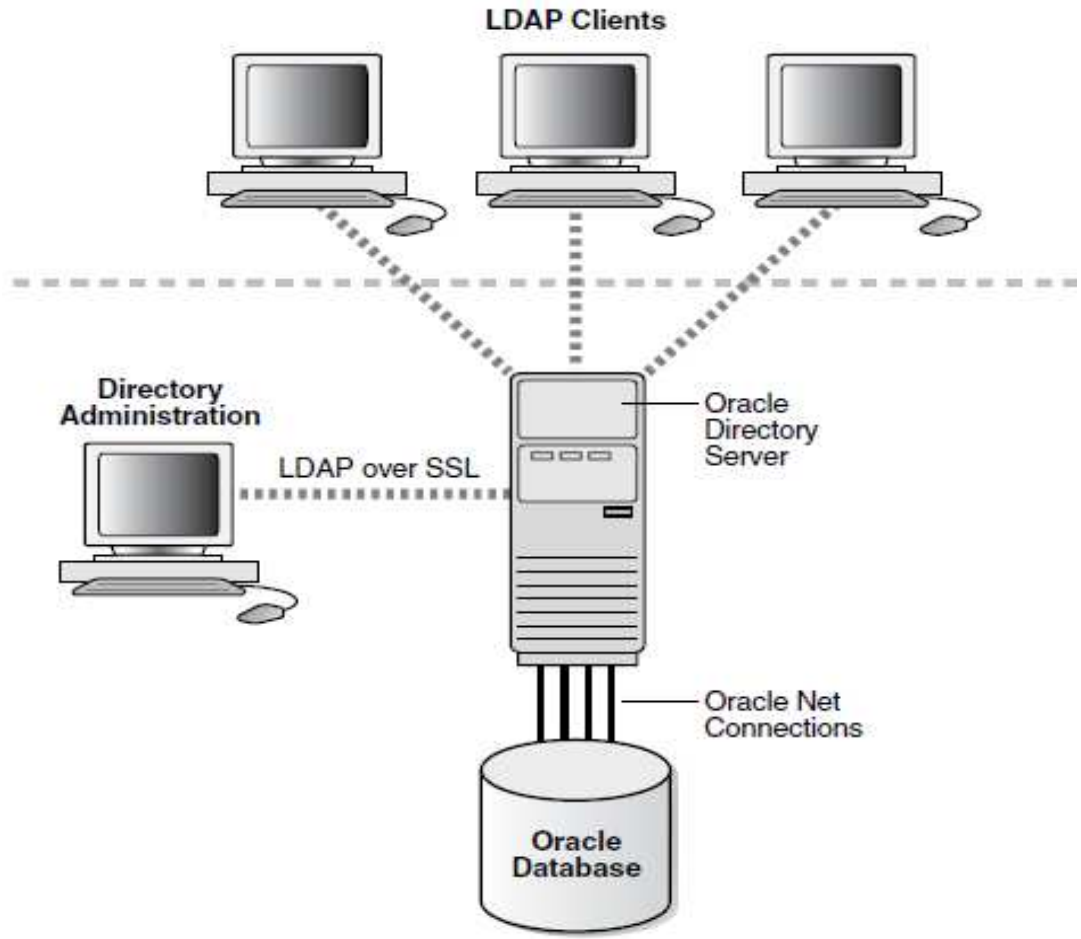
OPSS: Funktionalität



OPSS: Runtime



OPSS:
Oracle Directory Service



ODSM:
Oracle Directory Services Manager

ORACLE Directory Services Manager

Version Information

ODSM 11.1.1.2.0 OVD 11.1.1.2.0 Adapter Package 1

Adapters

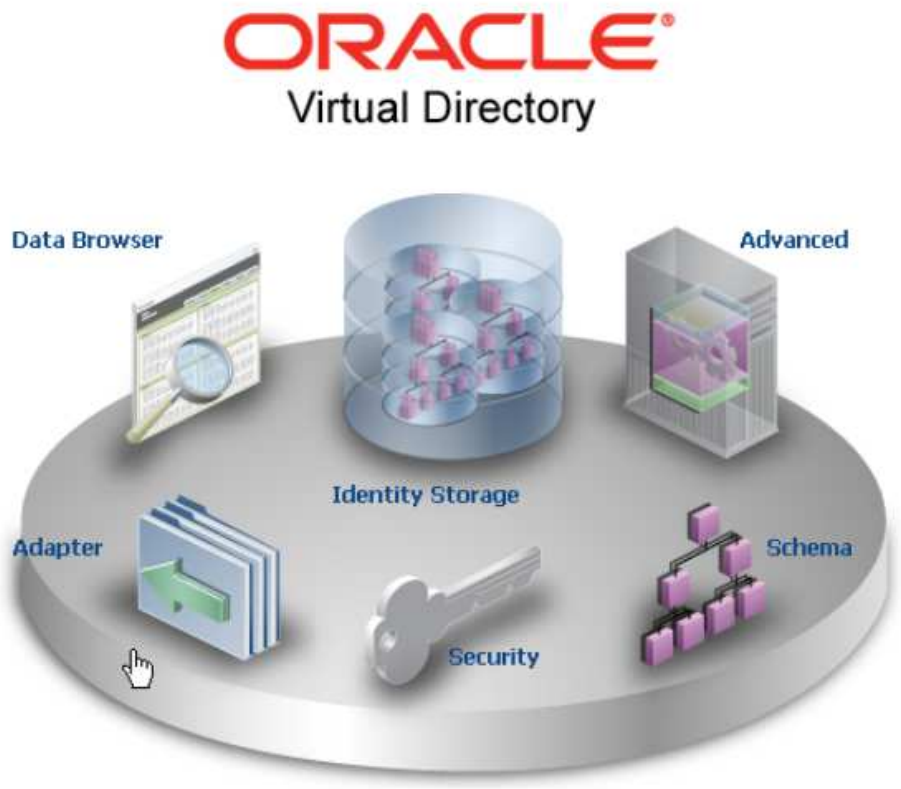
Name	Type	Visibility	Root
oid-stakb16	LDAP Adapter	Yes	dc=com

Listeners

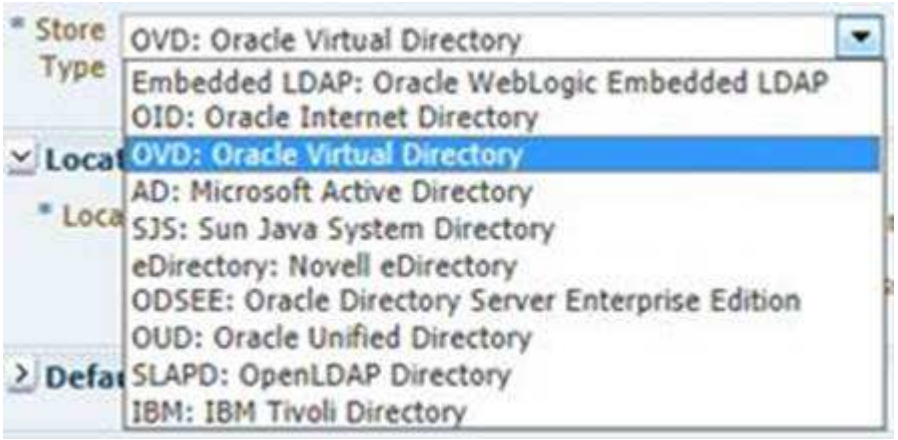
Name	Enabled	Type	Port	SSL Enabled
Admin Gateway	✓	ADMIN	8899	✓
LDAP SSL Endpoint	✓	LDAP	7501	✓
DSML Gateway	✗	HTTP	8080	✗
LDAP Endpoint	✓	LDAP	6501	✗

Navigation Tabs

- Data Browser — Navigate the virtual LDAP directory using the browse tree.
- Schema — Manage attributes and object classes.
- Security — Manage access control points.
- Advanced — Manage mapping templates, deployed mappings, global plug-ins, libraries, server views and configure wizards.
- Adapter — Manage adapters for LDAP, local store, custom, join, and database.



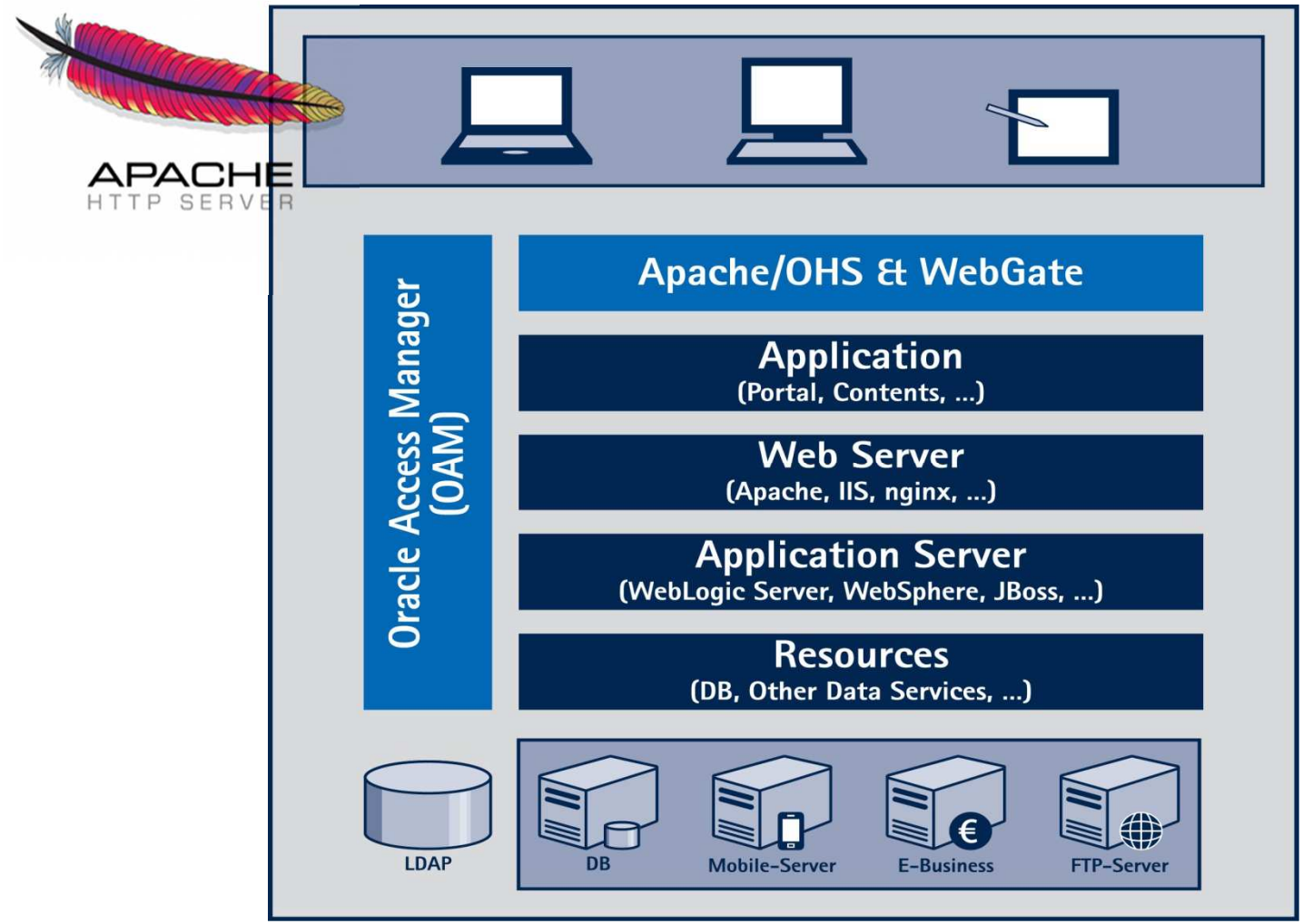
ODSM:
Oracle Directory Services Manager



- **LDAP**
- **OVD**
- **OID**
- **OUD**

OAM:
Oracle Access Management

Apache/ WebGate



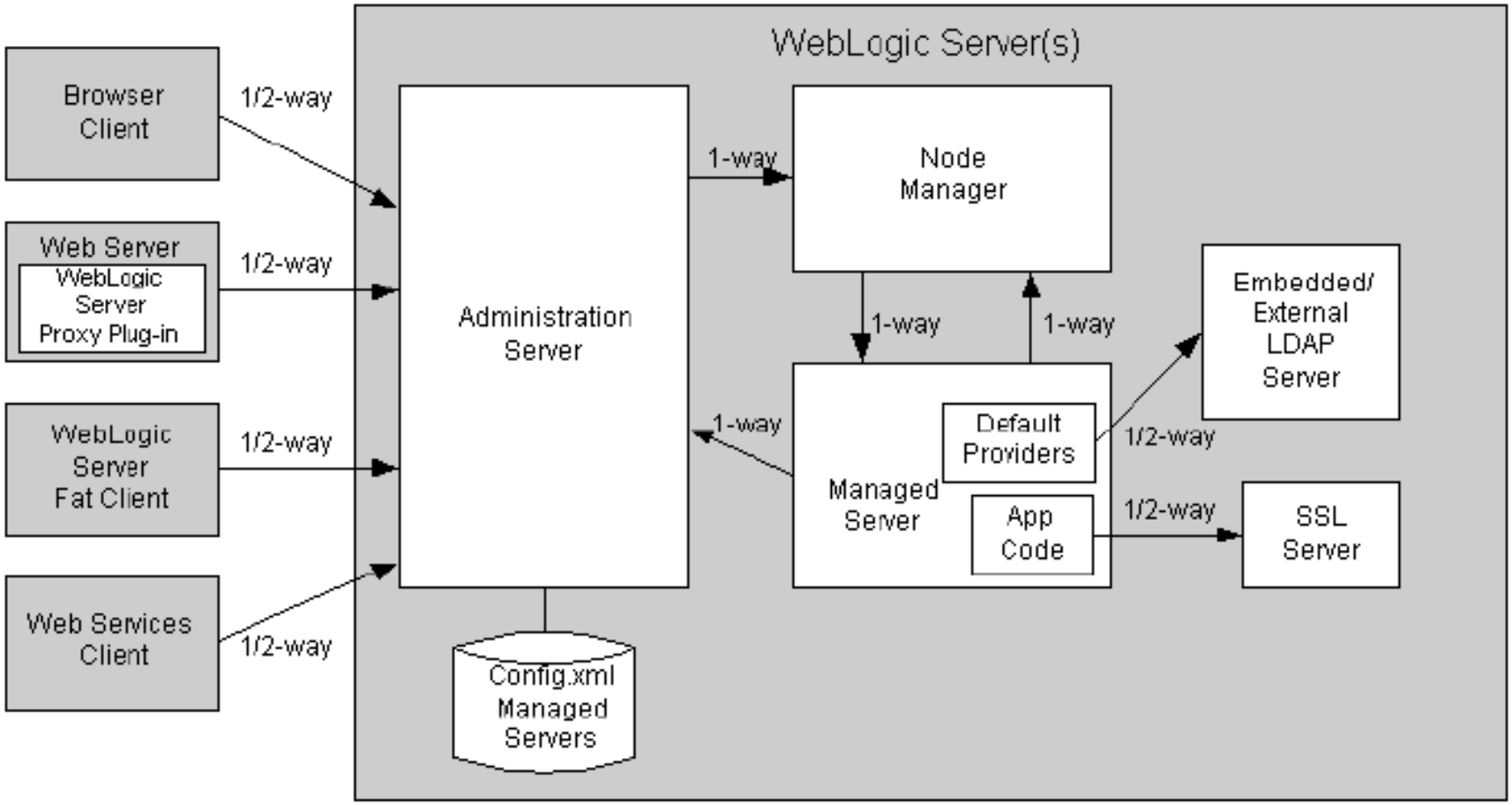
Agenda

1. Herausforderungen
2. Was verstehen wir unter IT-Sicherheit?
3. Oracle Ansatz: Konzept und Komponente
4. Sichere Kommunikation: SSL, PKI…
5. Forms Single-Sign-on Integration State of the Art
6. Zusammenfassung

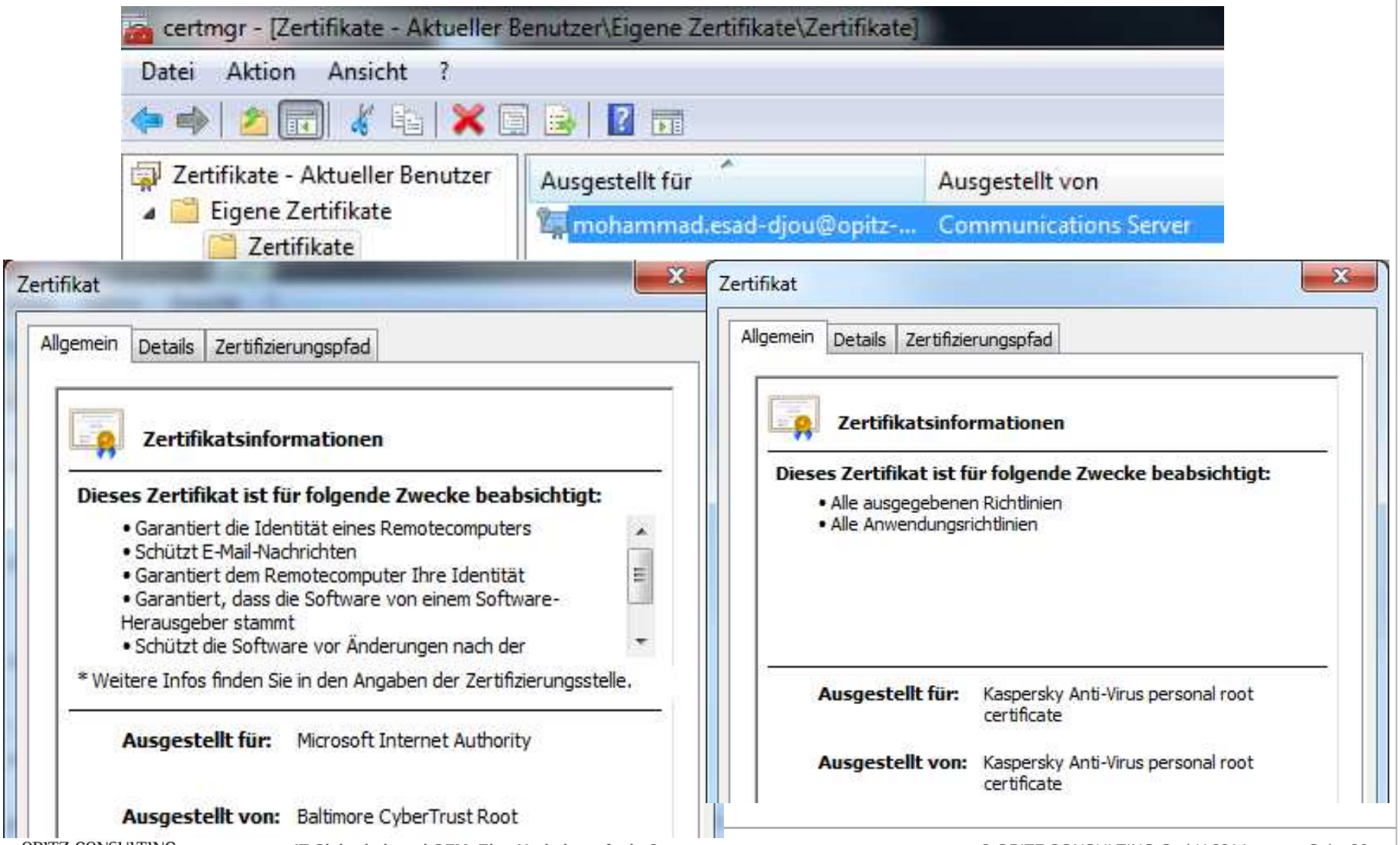
Sichere Kommunikation: SSL, PKI…

- Ein Mechanismus, dass die kommunizierenden Applikationen sich gegenseitig identifizieren und authentifizieren können.
- Verschlüsselung der ausgetauschten Daten von Anwendungen
- Technische Anforderungen:
  - Verschlüsselung
  - Zertifikate
  - öffentliche Schlüssel (Public Key)

SSL Authentication



SSL: Certificates

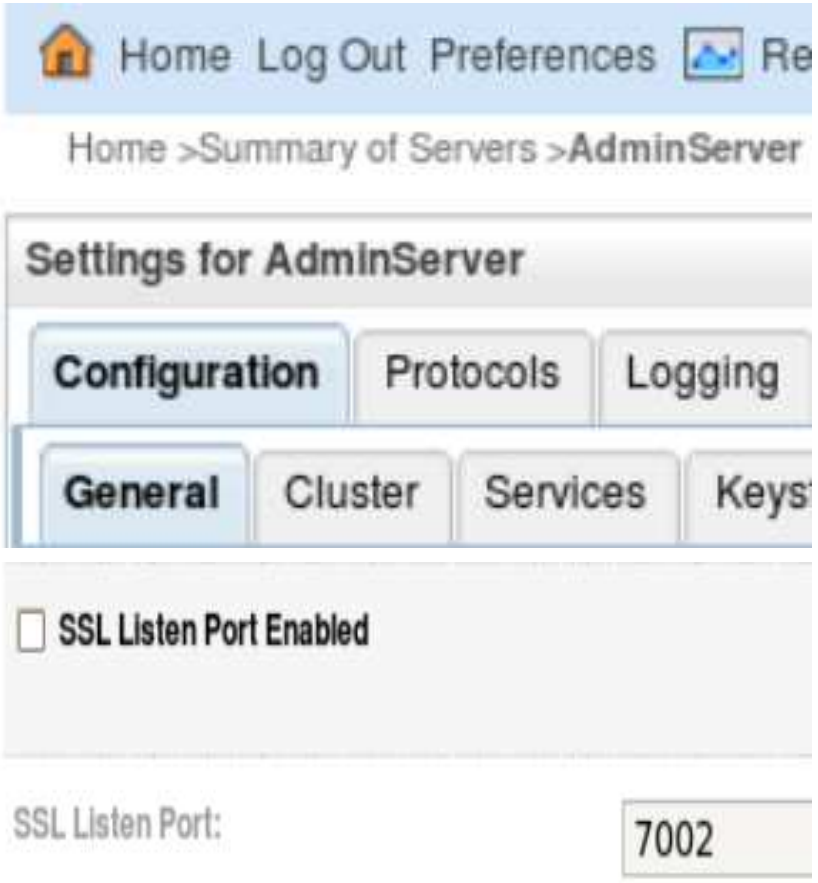


Trust and Identity

- **Identity: private key and digital certificate**
- **Trust: The trusted certificate authority (CA)**
- **Keytool generate the certificates**
- **A standard java keystore utility**
- **Keystore: A database of key material**
- **Types of Keystores: PKCS12, Sun's JKS**
- **A trust keystore contains the root and intermediate certificates which are trusted by the server.**

Trust and Identity

- **WebLogic default:**
  - **Demo Identity**
  - **Demo Trust**
- **Enable SSL port under the General Tab of the server**
- **Practice: Configure SSL on WLS with Custom Identity and Java Standard Trust**



SSL-Konfiguration auf WebLogic Server

1

Best Practice

```
keytool -genkeypair -alias server_cert -keyalg RSA -keysize 1024 -dname
"CN=Common, OU=Organisation, O=OC, L=Munich, ST=Bay,C=DE " -keypass
weblogic1234 -keystore server_keystore.jks -storepass weblogic1234
```

```
keytool -certreq -v -alias server_cert -file csr-for-myserver.pem -keypass
weblogic1234 -storepass weblogic1234 -keystore server_keystore.jks
```

```
keytool -import -v -noprompt -trustcacerts -alias ca-root-cert -file
rootcacert.cer -keystore server_keystore.jks -storepass weblogic1234
```

```
keytool -import -v -alias server_cert -file mycert.pem -keystore
server_keystore.jks -keypass weblogic1234 -storepass weblogic1234
```

SSL-Konfiguration auf WebLogic Server

2

Best Practice

keytool -list -v -keystore server_keystore.jks -storepass weblogic1234

Configure the keystore in WebLogic Server: Now login to WebLogic Server to configure these certificates.

In the left pane of the Console, expand Environment and select Servers.

Click the name of the server for which you want to configure the identity and trust keystores.

Check SSL Listen Port Enabled and if necessary set the value for SSL Listen Port <default 7002>

SSL-Konfiguration auf WebLogic Server

3

Best Practice

Select Configuration -> Keystores. Choose the Custom Identity and Java Standard Trust and fill in the below attributes:

Custom Identity Keystore: The fully qualified path to the identity keystore (e.g., path/server_keystore.jks).

Custom Identity Keystore Type: The type of the keystore. Generally, this attribute is Java KeyStore (JKS); if left blank, it defaults to JKS.

Custom Identity Keystore Passphrase: The password you will enter when reading or writing to the keystore (e.g., weblogic1234).

SSL-Konfiguration auf WebLogic Server

4

Best Practice

- Navigate to Home ->Summary of Servers ->AdminServer -> SSL
- Identity and Trust Locations: Keystores
- Private Key Alias: alias (The alias of the private key: in our case it is server_cert)
- Private Key Passphrase: weblogic1234
- Confirm Private Key Passphrase: weblogic1234
- Click SAVE

SSL-Konfiguration auf WebLogic Server

5

Best Practice

Now restart the server and try to access the Admin console

HTTPS port:https://<server name>:<server port>/console.

If you are able to access the console, that means you have successfully enabled SSL with the Keystore type as Custom Identity and Java Standard Trust.

keytool -alias <alias_name> -import -file rootcacert.cer -keystore trustkeystore.jks -storepass <Password>

Agenda

1. Herausforderungen
2. Was verstehen wir unter IT-Sicherheit?
3. Oracle Ansatz: Konzept und Komponente
4. Sichere Kommunikation: SSL, PKI…
5. Forms Single-Sign-on Integration State of the Art
6. Zusammenfassung

Forms Single-Sign-on Integration
Die Herausforderungen

- **Aufruf einer Forms Applikation ohne Login-Maske**
- **Initialer Aufruf der Applikation ohne Login-Dialog**
- **Sero-Single-sign-on**
- **Der Lösungsansatz :**

  → WNA (Windows Native Authentication)

Forms Single-Sign-on Integration
Die Herausforderungen

- **SSO-Integration der bestehenden Anwendungen**
  - Oracle Forms
  - Oracle Reports
  - Oracle Discoverer
- **Strategische SSO Integration**
- **Unternehmensweite Single Sign-on Lösung für weitere Anwendungen**
- **J2EE; SAP**
- **…**

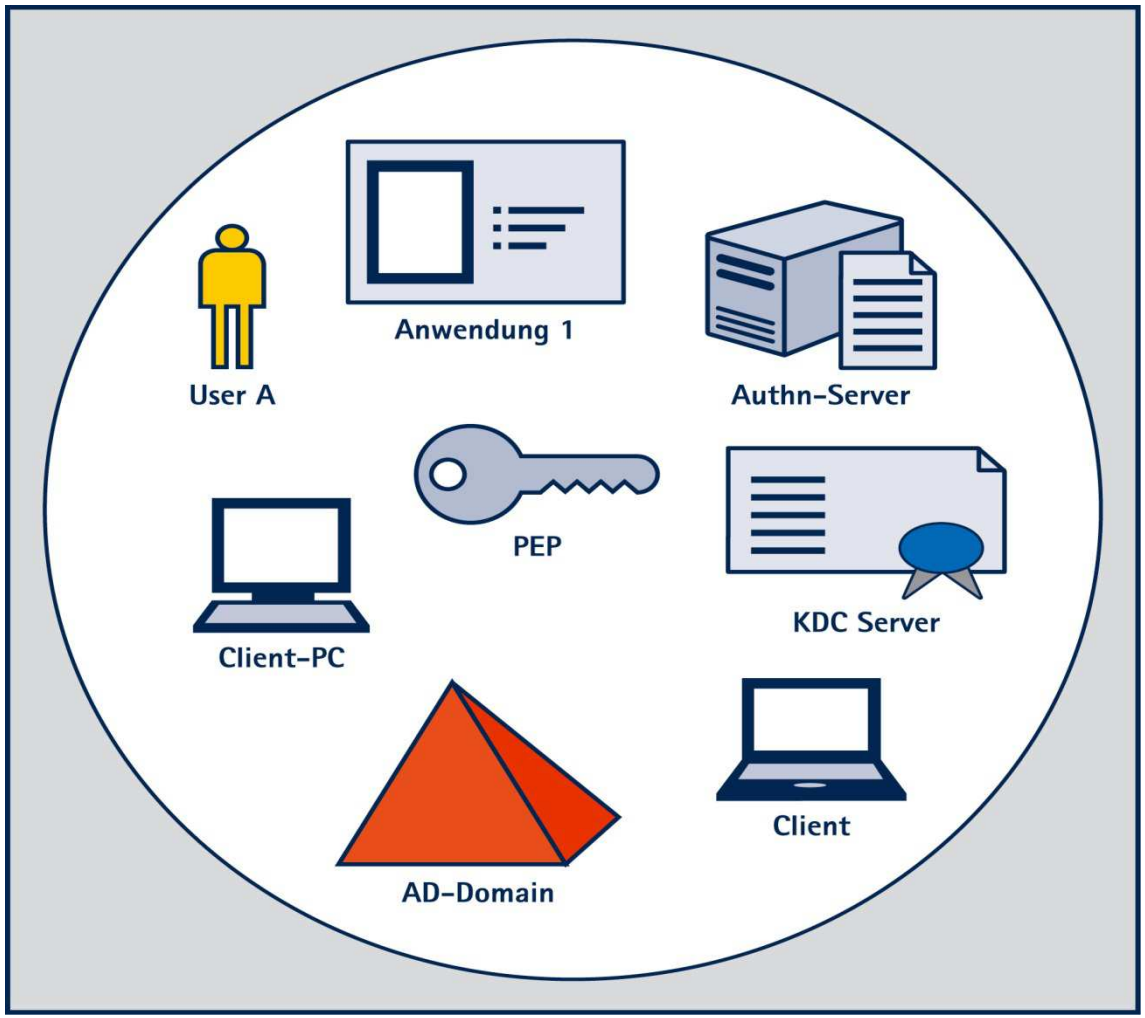
Betrachtung der Ausgangssituation

- **Die Komponenten Forms und Reports als auch die Discoverer Anwendung gehören zur Oracle Fusion Middleware.**
- **Bei einer SSO-Integration müssen die Rahmenbedingungen des Software Herstellers berücksichtigt werden.**
- **Zertifizierungsvorgaben**
- **Life Time Support**
- **Dokumentationen**
- **Lizenzkosten?**

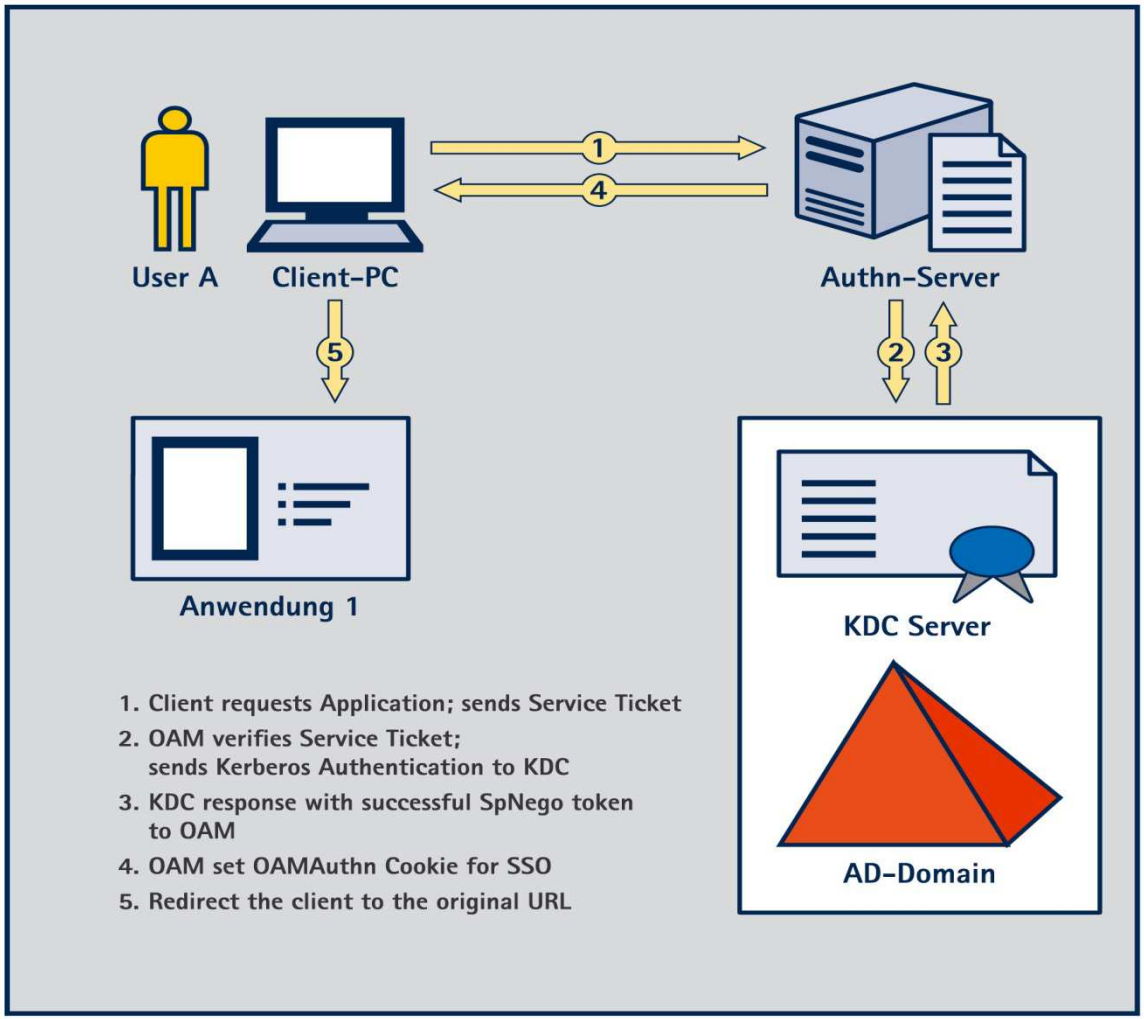
Dadurch resultieren Produktvorgaben

- **Oracle Access Manager 11g**
- **Strategisches Oracle Produkt für das Access Management**
- **Zugriffkontrolle, Authentifizierung und Single-Sign-on**
- **Nutzt Verzeichnisdienste z.B. OID**
- **Bietet verschieden Authentifizierungsmechanismen**
- **Basic Authentication, Kerberos, SSL**
- **Bietet Web SSO**

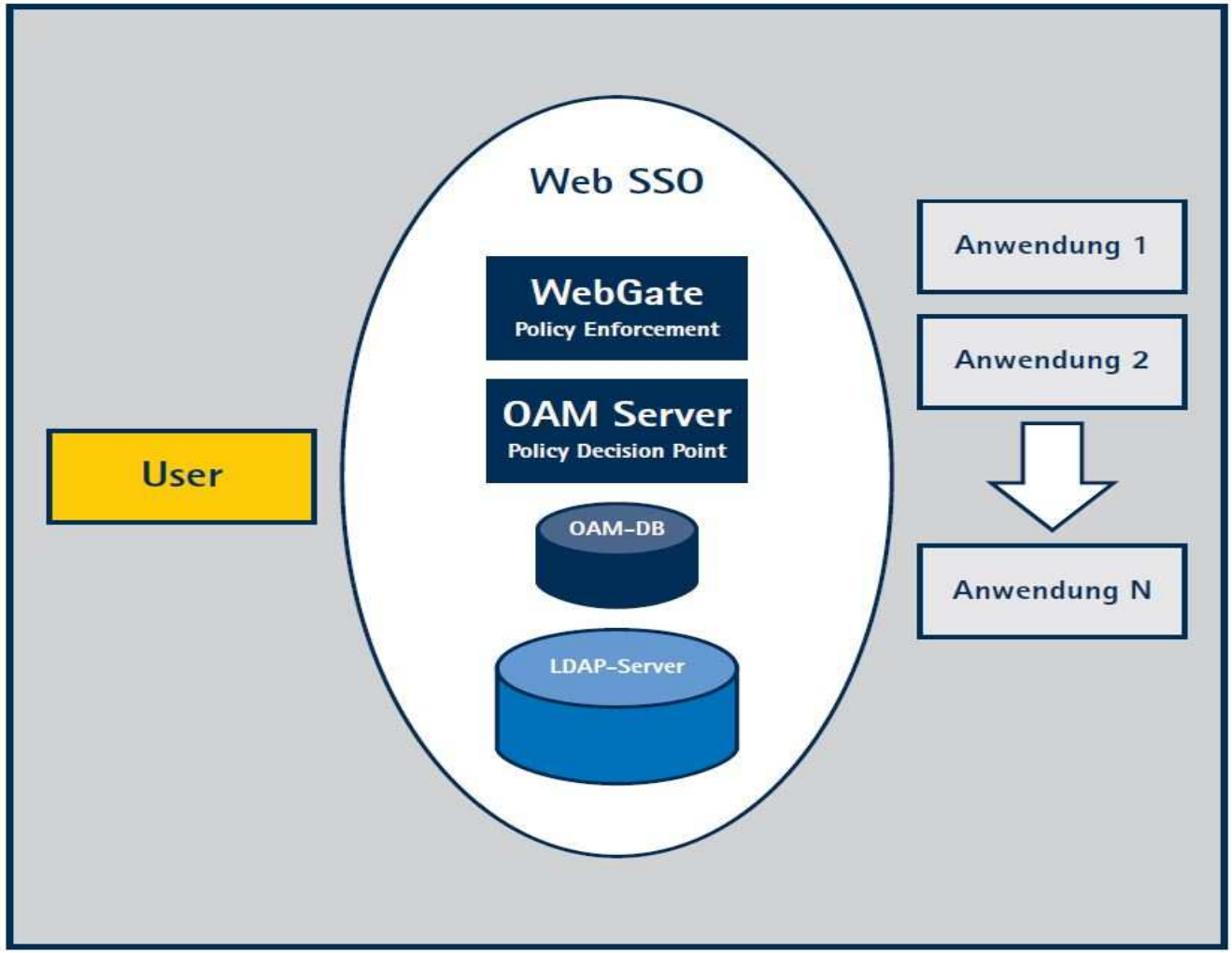
WNA – die Zutaten



WNA – Prinzip



Web-SSO-Infrastruktur



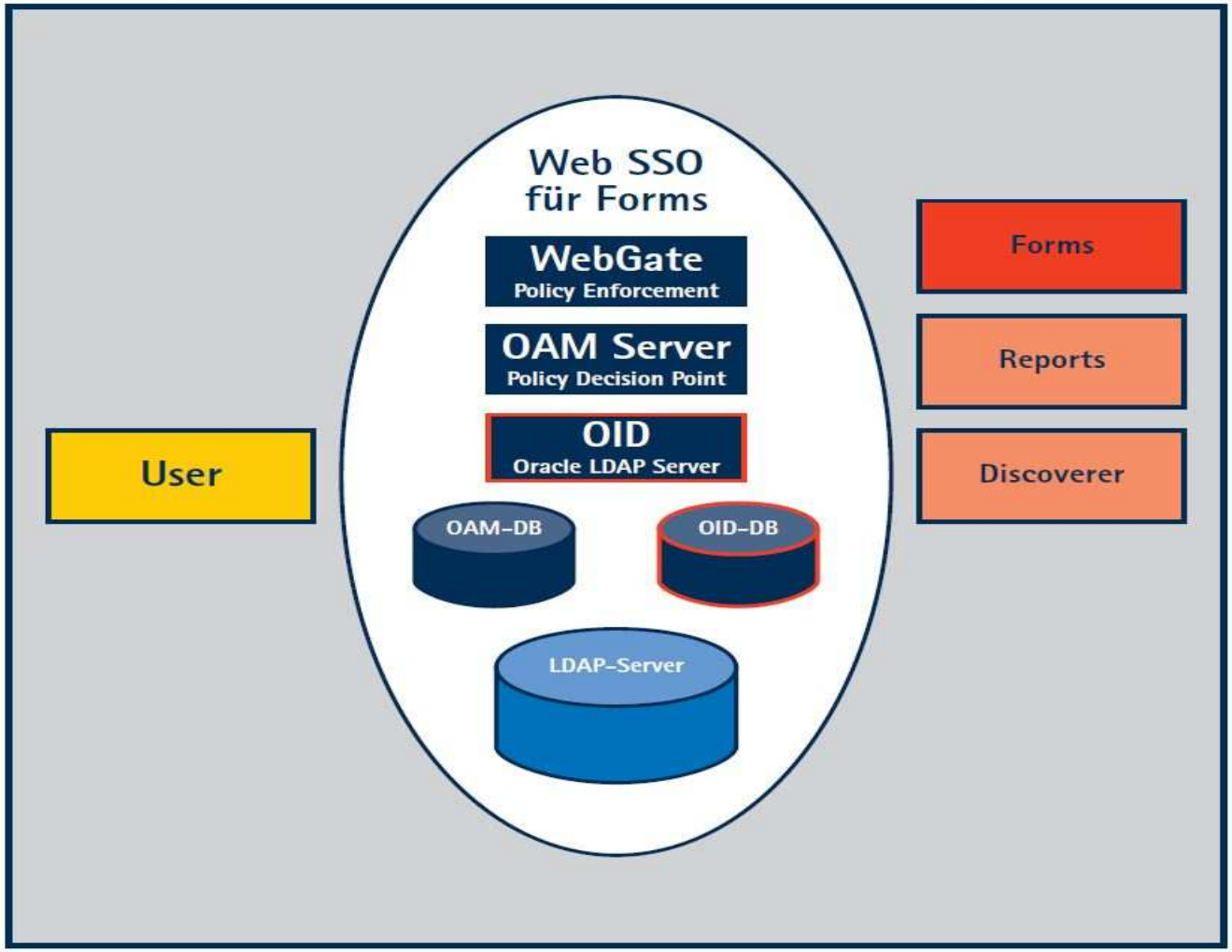
WEB-SSO Komponente OAM

- Der Oracle Access Manager gehört zum Produkt Bundle Identity and Access Management (IAM)
- Bestandteile dieser Installation sind
- WLS Admin Server →Policy Administration
- WLS Managed Server → Policy Decision Point
- WebGate → Policy Enforcement Point
- Als Identity Store kann OID genutzt werden

WEB-SSO Komponenten für Forms

- **Oracle Forms benötigt nach einer erfolgreichen Authentifizierung zusätzlich die notwendigen Informationen für die Anmeldung an der Datenbank.**
- **Diese Anmelde Informationen werden über den OID (Oracle Internet Directory) einem Oracle LDAP Server bereitgestellt.**

Web-SSO-Infrastruktur für Forms Integration



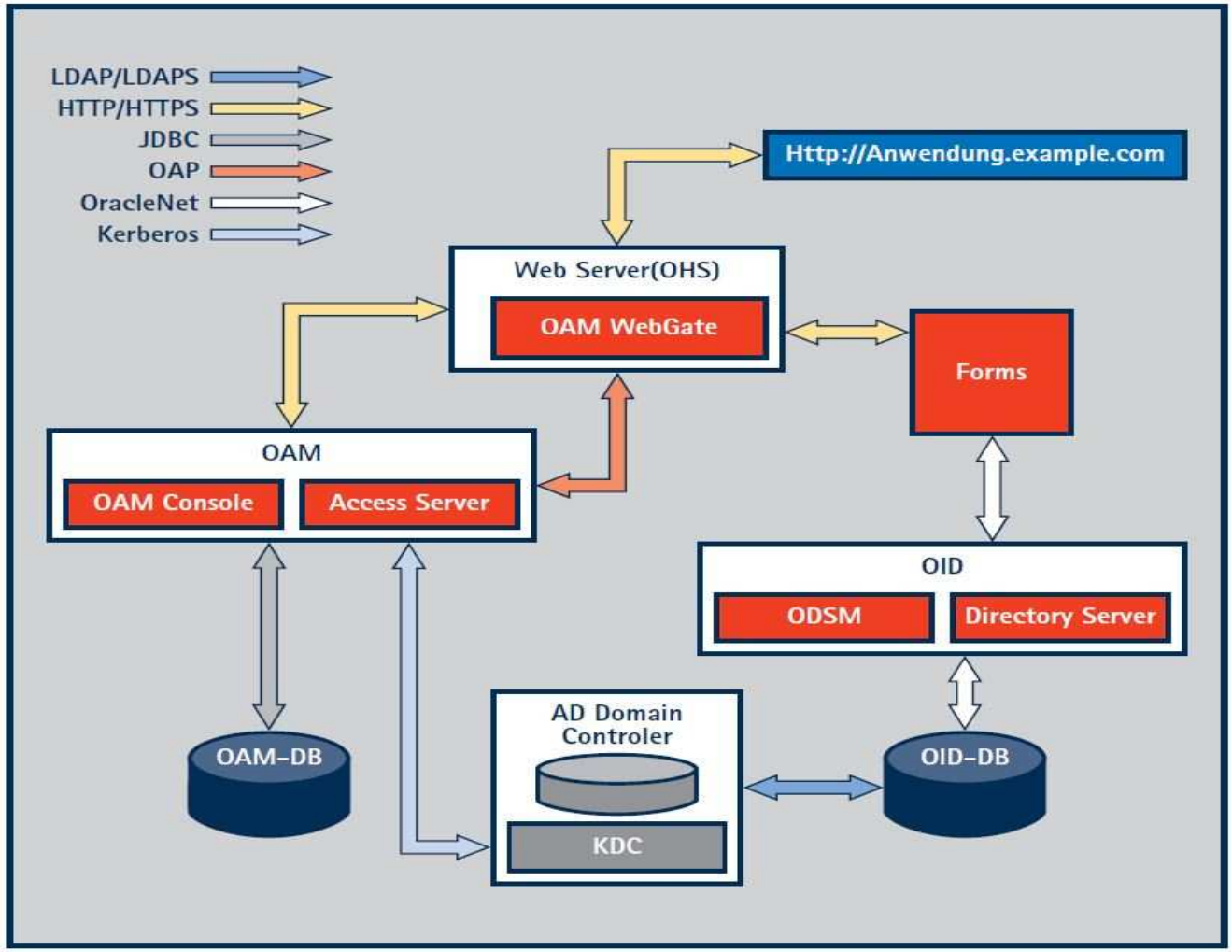
Oracle Internet Directory

- Der OID gehört zum Produkt Bundle Identity Management (IDM).
- Bestandteile dieser Installation sind
- WLS Domain → OID-Administration
- OID-Instance → LDAP Server Instanz
- OID DB → Datenbank Repository

Web-SSO-Komponenten für Forms Integration

- **Web Server**
  - Oracle HTTP Server
  - WebGate Plugin
- **OAM Domain**
  - Admin Server
  - OAM Console
  - Access Server
  - OAM-DB (DB-Repositories)
- **OID**
  - Oracle Directory Server
  - Admin Server
  - Oracle Directory Services Manager
  - OID-DB (DB-Repository)

Forms Web-SSO Integration



Agenda

1. Herausforderungen
2. Was verstehen wir unter IT-Sicherheit?
3. Oracle Ansatz: Konzept und Komponente
4. Sichere Kommunikation: SSL, PKI…
5. Forms Single-Sign-on Integration State of the Art
6. Zusammenfassung

Fragen und Antworten

Ansprechpartner bei OPITZ CONSULTING

Mohammad Esad-Djou, Solution Architect

OPITZ CONSULTING Deutschland GmbH
Mohammad.Esad-Djou@opitz-consulting.de
Telefon +49 89 680098-1400

Frank, Burkhardt, Senior Consultant

OPITZ CONSULTING Deutschland GmbH
Frank.Burkhardt@opitz-consulting.com
Telefon +49 89 680098-1400

youtube.com/opitzconsulting

@OC_WIRE

slideshare.net/opitzconsulting

xing.com/net/opitzconsulting