

IT-Symposium 2004 Bonn
Oracle Identity Managment
20.04.2004
1B03

ORACLE



Olaf Stullich
BU Database Technologies
Oracle Deutschland GmbH

ORACLE

Sicherheit aller Applikationen

Ein User- ein Account- ein Passwort

Kosten für Passwort- und User Management	
Forrester	US\$ 200 pro Jahr / User
Gartner	US\$ 300 pro Jahr / User
IDC	US\$ 340 pro Jahr / User

ORACLE

Was ist Identity Management?

Identity Management bezeichnet den Prozeß bei dem:

- Benutzeridentitäten angelegt und verwaltet werden
- Anwender automatisiert angelegt werden
- Benutzerrollen, Privilegien & Berechtigungen verwaltet werden
- Administratoren Verantwortlichkeiten delegieren
- Administratoren Anwendungen leicht & sicher verteilen
- Anwender selbständig Passwörter und Präferenzen ändern können
- Benutzer einen Single Sign-On Zugang haben

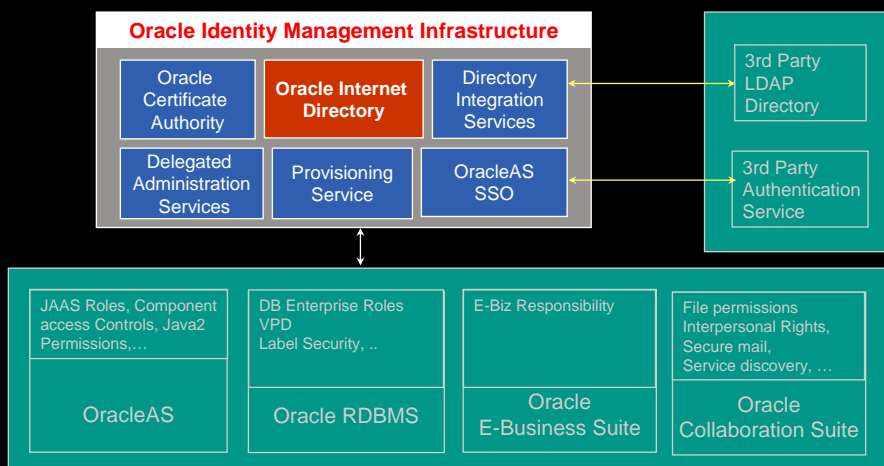
ORACLE

Identity Management Vorteile

- **Kostenersparnis**
 - Zentrales Benutzermanagement reduziert Administrationskosten
 - Leichter zu automatisieren
 - Weniger Fehler anfällig
- **Erhöhte Sicherheit**
 - Keine fragmentierte Sicherheit
- **Erhöhte Benutzerakzeptanz**
 - Single Password und Single Sign-on
 - Personalisierung
 - Delegierte Administration und Self-service

ORACLE

Oracle Identity Management



ORACLE

Was sind Verzeichnisdienste ?

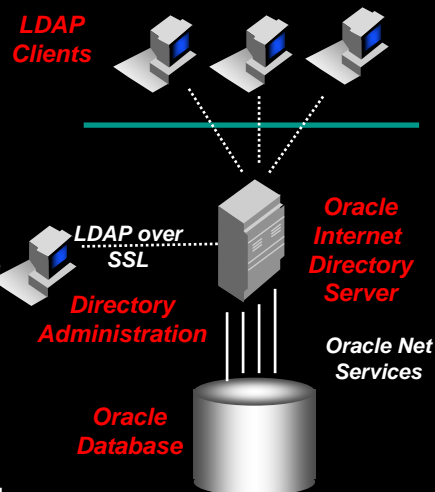
- flexible, spezialisierte und verteilte Datenhaltung
- Speicherung und Suche Eintrags-orientierter Informationen für unterschiedliche Anwendungen



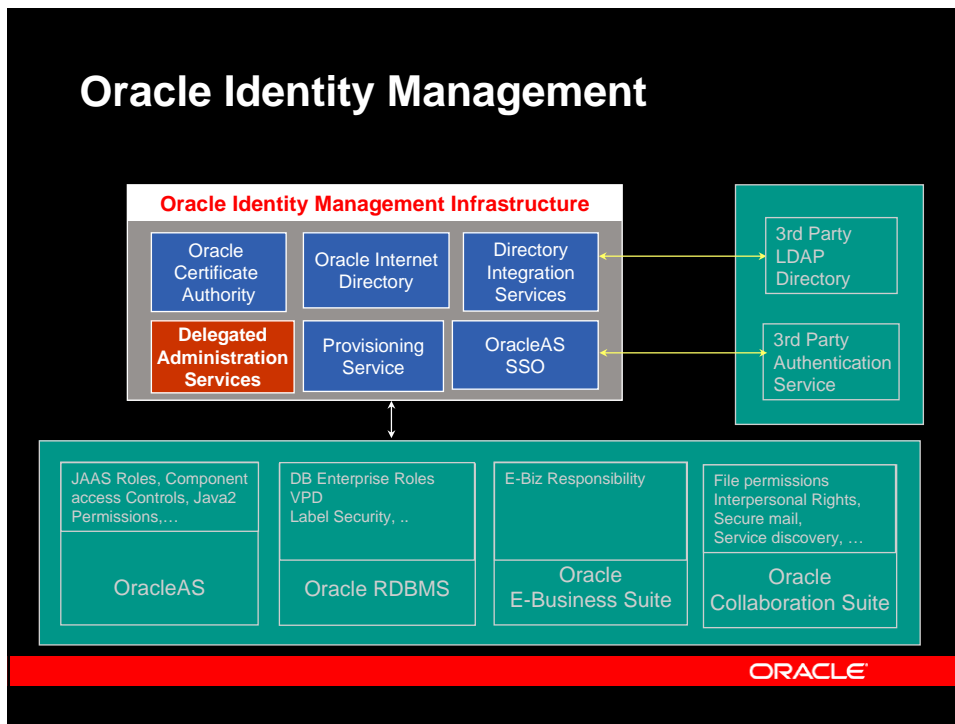
ORACLE

Oracle Internet Directory

- Standard basierend
 - Native LDAPv3 Implementierung
 - Integration mit der Oracle System Management Umgebung
- Skalierbarkeit
 - "unbeschränkte" Anzahl von Entries auf einem Server
 - 1000'de gleichzeitiger Client Zugriffe
- Hochverfügbarkeit
 - Multimaster-Replikation durch Benutzung von Oracle Advanced Symmetric Replication
 - Oracle Real Application Cluster
- Sicherheit
 - Hochentwickeltes Sicherheits-Modell



ORACLE



Delegated Administration Services

- Einheitliche Schnittstelle zur Directory Datenverwaltung
 - **Administrator**: unterstützt Benutzer und anwendungsspezifische Berechtigungsverwaltung
 - **Endanwender**: ändern von Passwörtern, Präferenzen, Profilen etc.

Delegated Administration Service

Oracle

Benutzer anlegen

Oracle

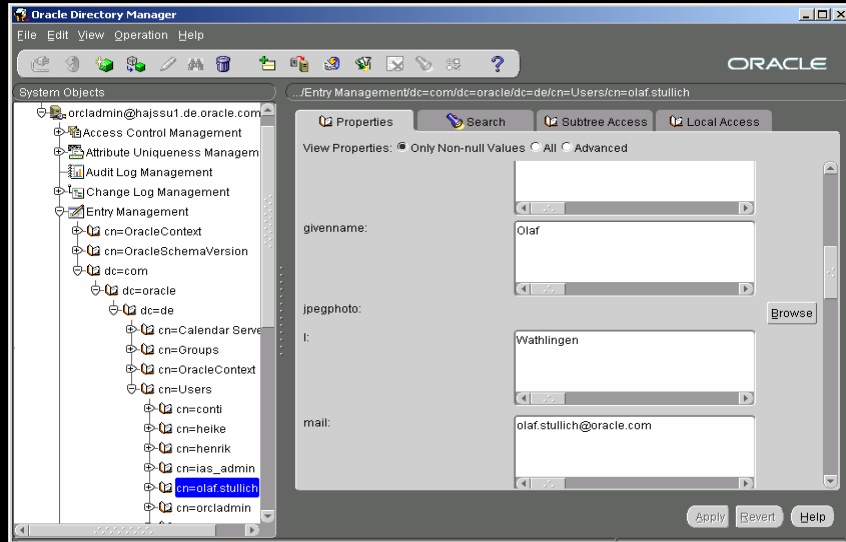
Benutzerprofil

ORACLE

OID Admin Console

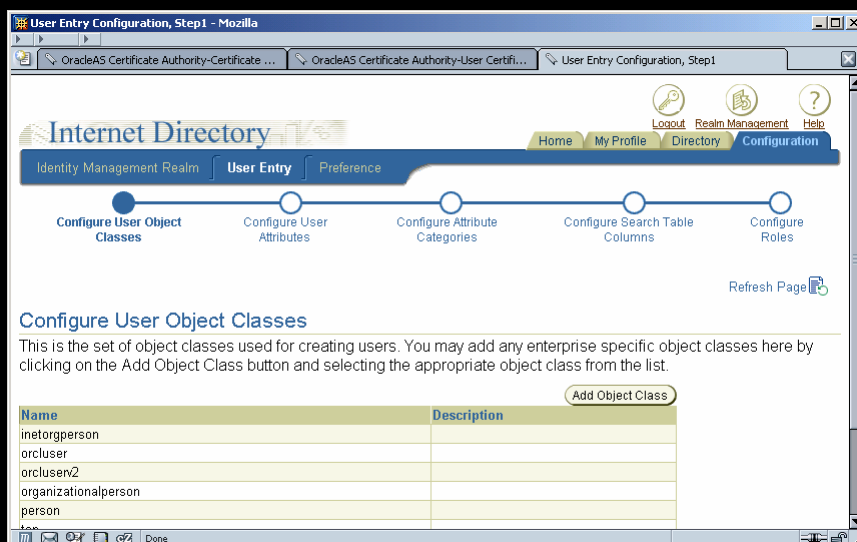
ORACLE

OID Admin Console



ORACLE

Benutzer Einstellungen



ORACLE

Disable user accounts

The screenshot shows a web browser window titled 'Enabled Account List - Mozilla'. The page is part of the Oracle Internet Directory. It features a search bar with the text 'Search for enabled user accounts' and a 'Go' button. Below the search bar are tabs for 'Unlock Accounts', 'Enable Accounts', and 'Disable Accounts'. A paragraph of text explains that administrators can search and view enabled user accounts and disable them. Below this is a table with the following data:

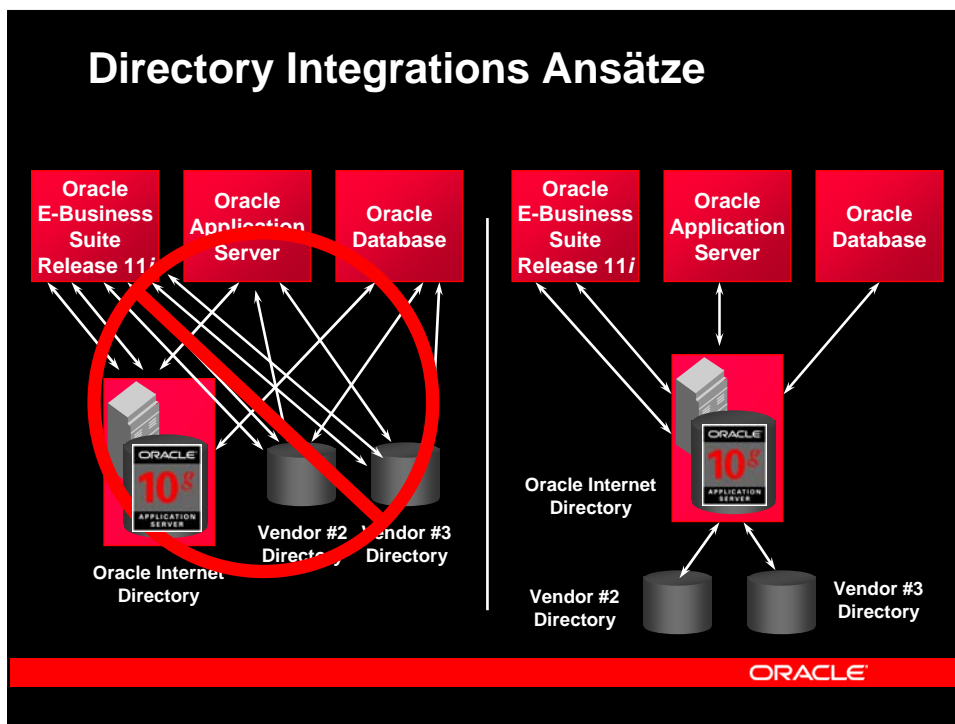
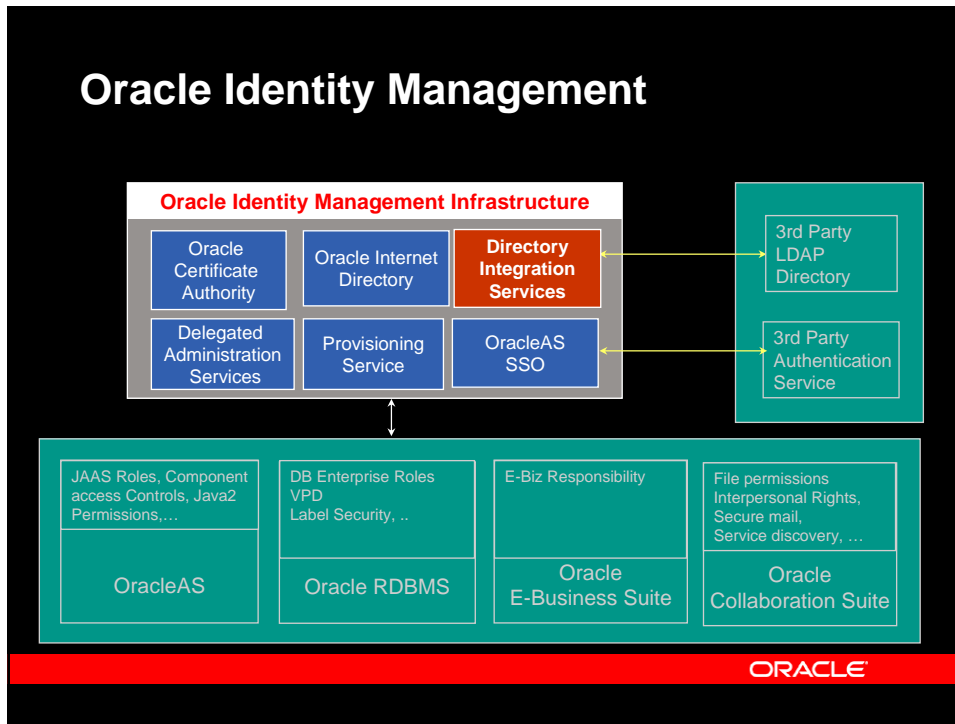
Select Name	Email Address
<input type="radio"/> Guest	
<input type="radio"/> IUSR_OSTULLIC-W2KSRV	
<input type="radio"/> IWAM_OSTULLIC-W2KSRV	
<input type="radio"/> markus	markus.michalewicz@oracle.com
<input type="radio"/> olaf.ad	
<input checked="" type="radio"/> olaf.stulich	olaf.stulich@oracle.com
<input type="radio"/> orcladmin	orcladmin
<input type="radio"/> ostullic	olaf.stulich@oracle.com

ORACLE

Demo

Delegated Administration Service

ORACLE



mySap.com Zertifizierung

- SAP WAS 6.20
- SAP LDAP Connector 2.1
- OID 9.2



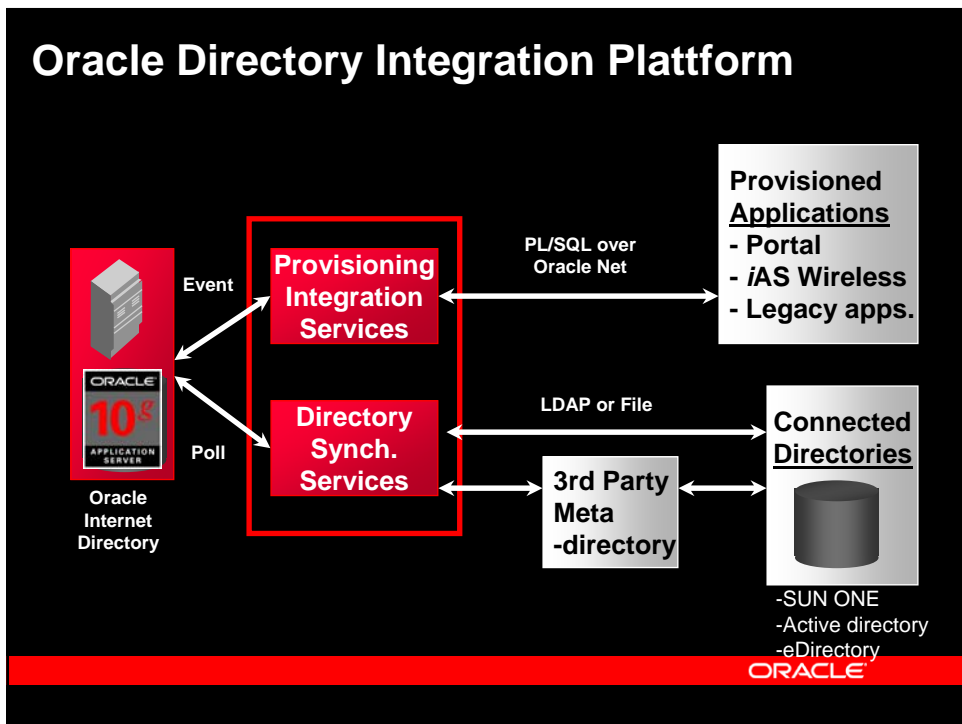
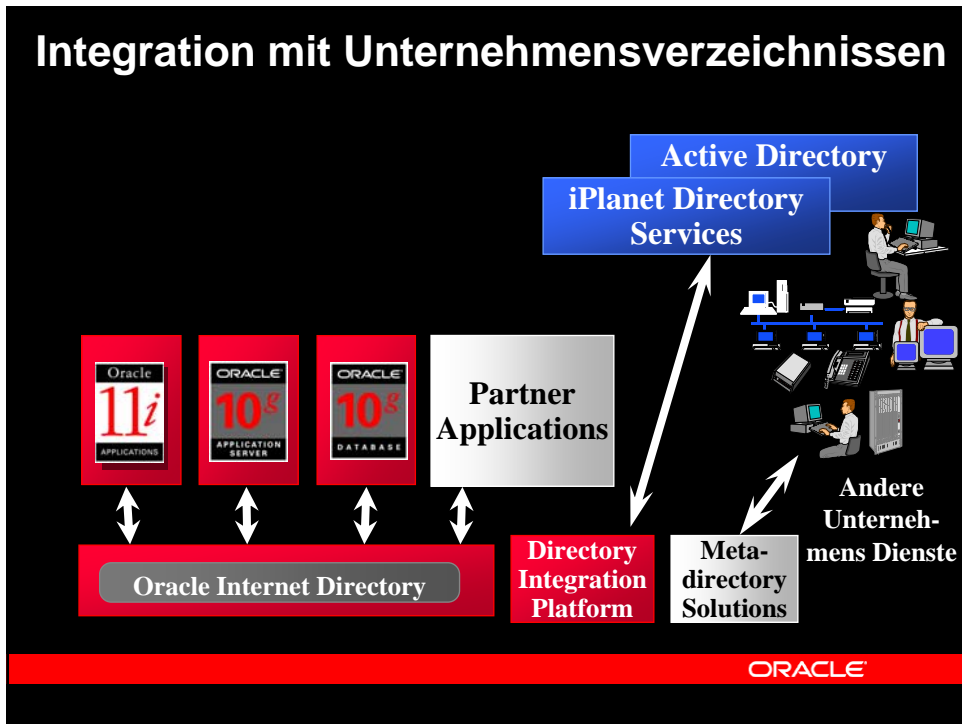
ORACLE

Integration mit Unternehmensverzeichnissen

Enterprise Directory Services

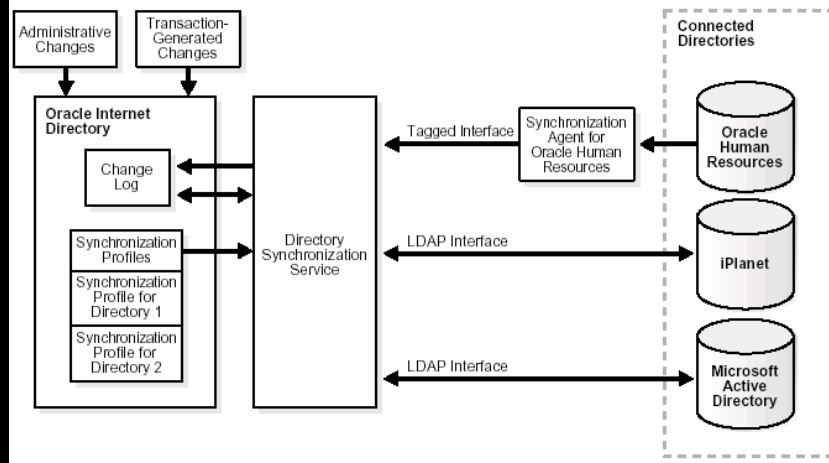


ORACLE



Directory Synchronisation

Figure 31-2 Interactions of the Oracle Directory Synchronization Service



ORACLE

Directory Synchronization Service

- Der Synchronization Integration Service koordiniert die Änderungen zwischen den Directoryservern und dem zentralen OID-Server in einem Unternehmen
- Synchronisation stellt die Konsistenz der Daten in einem Unternehmen sicher
- Für jedes angeschlossene Directory muß eine eigenes Synchronisationsprofil angelegt werden

ORACLE

Connector

- Ein Connector ist eine vorkonfigurierte Lösung zwischen einem OID-Server und anderen Verzeichnissen
- Ein Connector besteht aus einem Connector Profile->Directory Integration Profile
- Ein Connector Profile enthält alle Informationen um Daten zwischen einem OID-Server und verbundenen Verzeichnissen zu synchronisieren

ORACLE

Synchronization Agent

- Ein Agent ist ein spezielles Programm, das Daten zwischen einem OID und Servern mit anderen Datenformaten synchronisiert
- Agenten konvertieren die Daten in ein Zwischenformat bevor sie in das native Verzeichnisformat umgesetzt werden

ORACLE

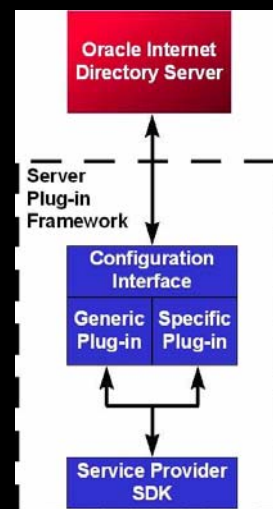
Directory Synchronization Profiles

- Es werden separate Synchronisation Profile für jede Synchronisationsrichtung benötigt
- Synchronisationsprofile unterstützen folgende Interface:
 - PL/SQL
 - LDAP
 - Tagged
 - LDIF
- Der Directory Synchronization Service (DSS) arbeitet periodisch das Synchronisation Profile ab

ORACLE

Oracle Internet Directory Plug-In Framework

- Neue Funktionalität mit Oracle9i Application Server R2
- Plug-in`s sind PL/SQL packages
- Erlaubt Aufruf Benutzerdefinierter Operationen
- Aufruf bei LDAP Kommando Ausführung
 - ldapbind, ldapadd, ldapmodify, ldapcompare, ldapsearch, ldapdelete



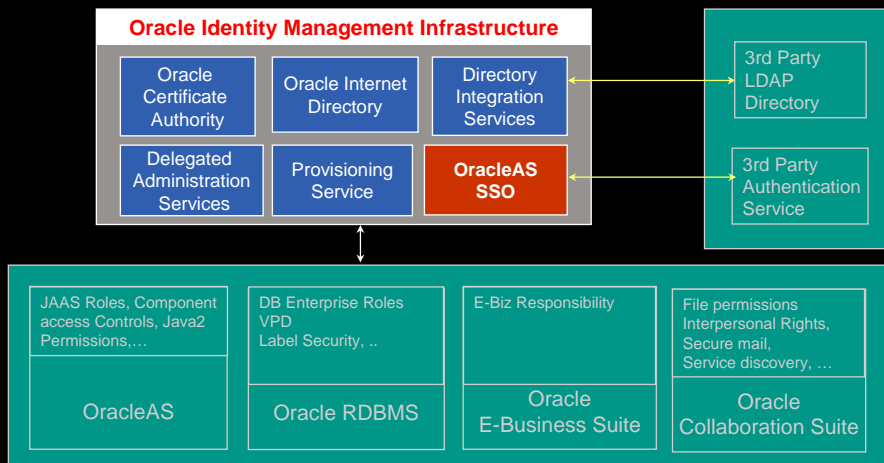
ORACLE

Unterstützte Plug-In Operationen

- **Pre-Operation**
 - Vor Ausführung der LDAP Operation
 - Z.B. Überprüfung der Daten bevor diese von LDAP Operationen genutzt werden
- **Post-Operation**
 - Nach Durchführung einer LDAP Operation
 - Z.B. Protokollierung und Benachrichtigung
- **When-Operation**
 - in Ergänzung der Standardoperationen
 - z.B. erweitert bestehende Funktionalität
 - When-operation (Add-on / Replace)

ORACLE

Oracle Identity Management



ORACLE

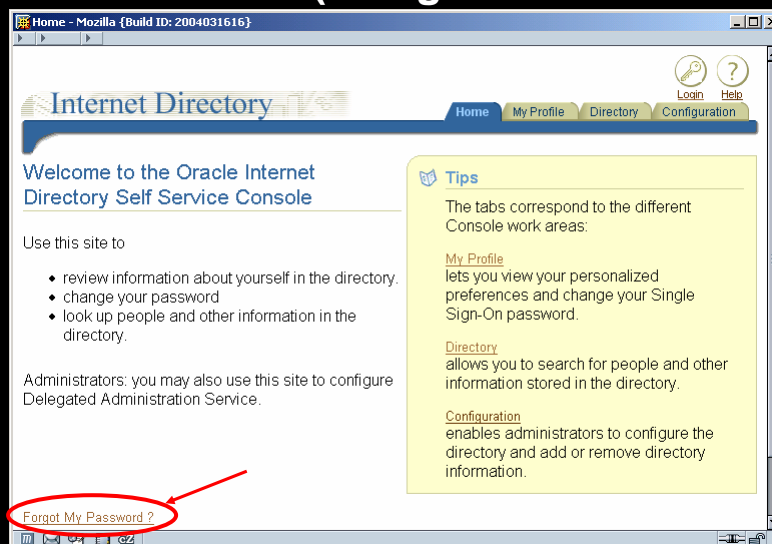
Sicherheit aller Applikationen

Ein User- ein Account- ein Passwort

Kosten für Passwort- und User Management	
Forrester	US\$ 200 pro Jahr / User
Gartner	US\$ 300 pro Jahr / User
IDC	US\$ 340 pro Jahr / User

ORACLE

Password Reset 1 (Delegated Admin Service)



ORACLE

Password Reset 2 (Delegated Admin Service)

The screenshot shows a web browser window titled "Self Reset Password, Step1 - Mozilla {Build ID: 2004031616}". The page header includes "Home" and "Help" links. A progress bar at the top indicates three steps: "Confirm Identity" (active), "Confirm Additional Personal Information", and "Reset SSO Password". The main heading is "Reset My Single Sign-On Password". Below it, the sub-heading is "Confirm Identity". The instructions state: "Your identity needs to be confirmed by entering your Single Sign-On user name and name of the company you are associated with. Click on Next to continue." A text input field labeled "User Name" contains the text "olaf.stullich". At the bottom right, there are "Cancel" and "Next" buttons, with "Step 1 of 3" in between. At the bottom center, there are "Home" and "Help" links. The browser's status bar at the bottom shows "Done".

ORACLE

Password Reset 3 (Delegated Admin Service)

The screenshot shows a web browser window titled "Self Reset Password, Step2 - Mozilla {Build ID: 2004031616}". The page header includes "Home" and "Help" links. A progress bar at the top indicates three steps: "Confirm Identity", "Confirm Additional Personal Information" (active), and "Reset SSO Password". The main heading is "Reset My Single Sign-On Password". Below it, the sub-heading is "Confirm Additional Personal Information". The instructions state: "In order to reset your password, you must correctly enter additional information associated with your account." A text input field labeled "Wie heisst Ihre Lieblingshunderasse:" contains the text "Labrador". At the bottom right, there are "Cancel", "Back", and "Next" buttons, with "Step 2 of 3" in between. At the bottom center, there are "Home" and "Help" links. The browser's status bar at the bottom shows "Done".

ORACLE

Password Reset 3 (Delegated Admin Service)

Self Reset Password, Step3 - Mozilla {Build ID: 2004031616}

Reset My Single Sign-On Password

Confirm Identity Confirm Additional Personal Information **Reset SSO Password**

Reset SSO Password

You need to enter new password to override your original SSO password. Click on Next to continue.

New Password

Confirm New Password

Cancel Back Step 3 of 3 Finish

[Home](#) | [Help](#)

ORACLE

Password Reset 4 (Delegated Admin Service)

Finish Self Reset Password - Mozilla {Build ID: 2004031616}

Reset My Single Sign-On Password

Reset SSO Password

Successfully reset your password.

OK

[Home](#) | [Help](#)

ORACLE

Demo

Delegated Administration Service

Password Reset

ORACLE

Definitionen

- **Single Sign-on (SSO)**
- ein Passwort
- **Single Station Administration (SSA)**
- ein Verwaltungswerkzeug
- **Single Source of Control (SSC)**
- zentrale Datenverwaltung

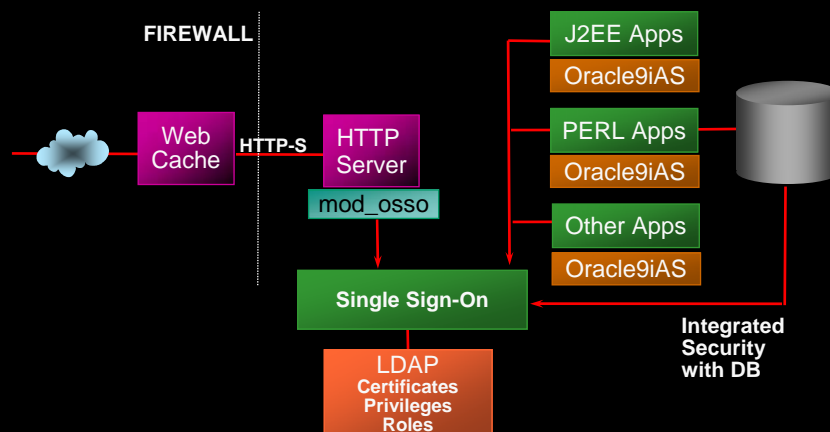
ORACLE

Oracle SSO Server

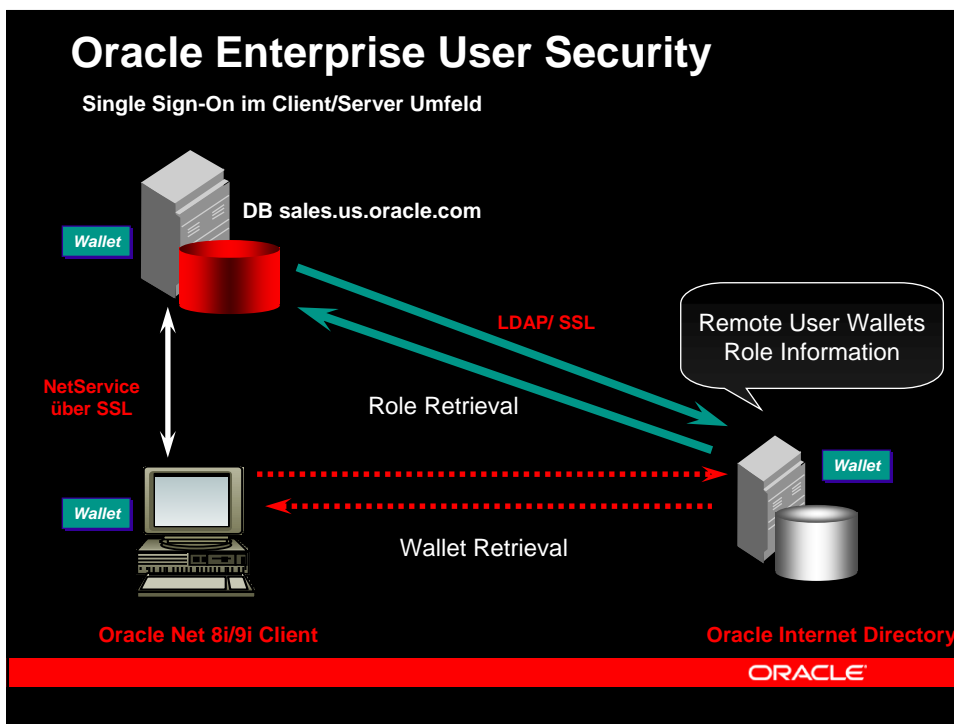
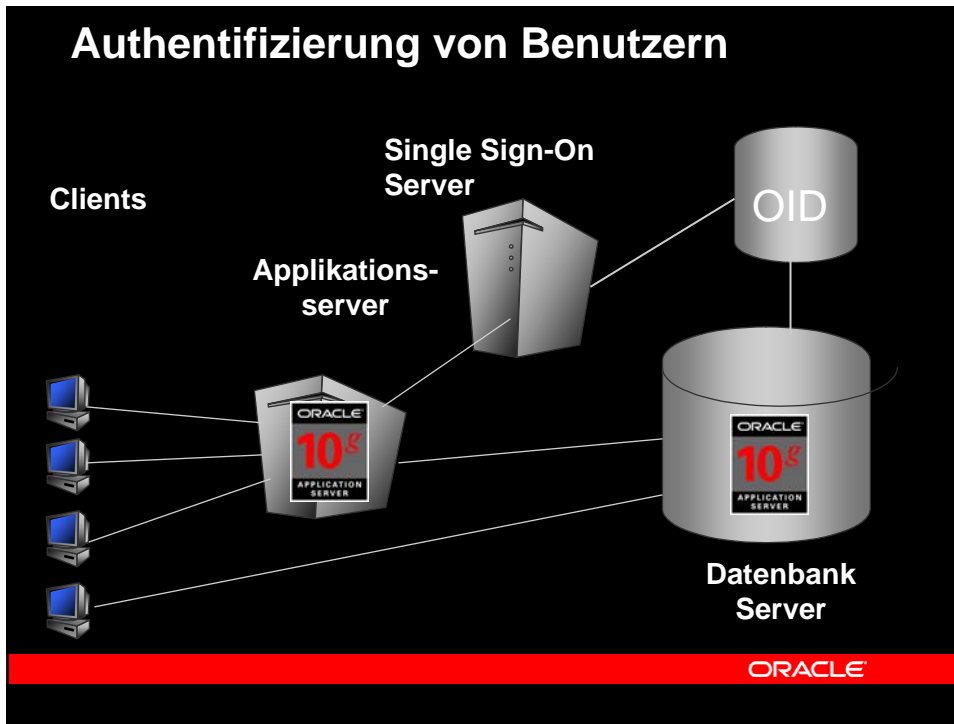
- Kernkomponente der Oracle's Web SSO Technologie
- Authentifiziert Benutzer und reicht deren Identität sicher an Partner-Anwendungen weiter
- Fordert den Benutzer zur Eingabe eines Namens und Passwortes auf:
 - beim erstmaligen Systemzugriff innerhalb einer vorgegebenen Zeit
 - verifiziert das Passwort

ORACLE

Architektur



ORACLE



Bsp SSL based authentication

```
ostullic's X desktop (hajssu1.de.oracle.com:1)
$ sqlplus /@ora9202ssl
SQL*Plus: Release 9.2.0.2.0 - Production on Thu Jun 26 16:54:37 2003
Copyright (c) 1982, 2002, Oracle Corporation. All rights reserved.

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.2.0 - Production
JServer Release 9.2.0.2.0 - Production

SQL> show user
USER is "GUEST"
SQL> SELECT SYS_CONTEXT ('USERENV', 'EXTERNAL_NAME') FROM DUAL;

SYS_CONTEXT('USERENV','EXTERNAL_NAME')
-----
cn=ostullic,cn=users,dc=de,dc=oracle,dc=com

SQL> select * from session_roles;

ROLE
-----
CONNECT
RESOURCE
EMPROLE
```

ORACLE

Beispiel Login username/pwd

```
Oracle SQL*Plus
Datei Bearbeiten Suchen Optionen Hilfe
Oracle9i Enterprise Edition Release 9.2.0.2.0 - Production
JServer Release 9.2.0.2.0 - Production

SQL> show user
USER ist "GUEST"
SQL> SELECT SYS_CONTEXT ('USERENV', 'CURRENT_USER') FROM DUAL;

SYS_CONTEXT('USERENV','CURRENT_USER')
-----
GUEST

SQL> SELECT SYS_CONTEXT ('USERENV', 'EXTERNAL_NAME') FROM DUAL;

SYS_CONTEXT('USERENV','EXTERNAL_NAME')
-----
cn=ostullic,cn=users,dc=de,dc=oracle,dc=com

SQL> select * from session_roles;

ROLE
-----
CONNECT
RESOURCE
EMPROLE

SQL>
```

Anmeldung

Benutzername:	<input type="text" value="ostullic"/>
Kenntwort:	<input type="password" value="*****"/>
Host-Zeichenfolge:	<input type="text" value="ORA9202_HAJSSU1"/>

ORACLE

Beispiel

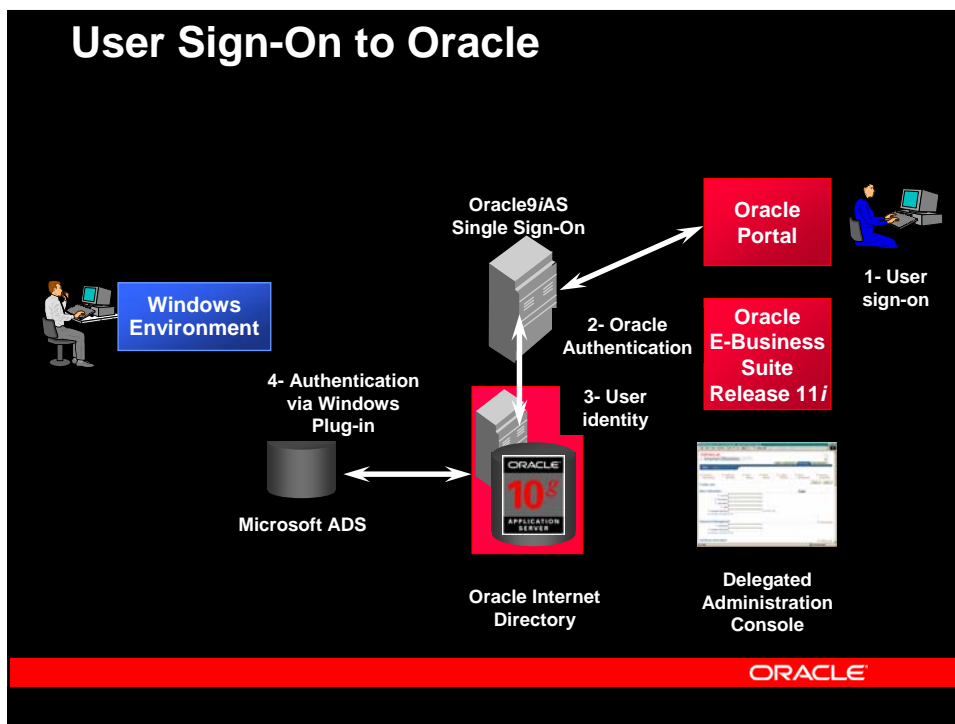
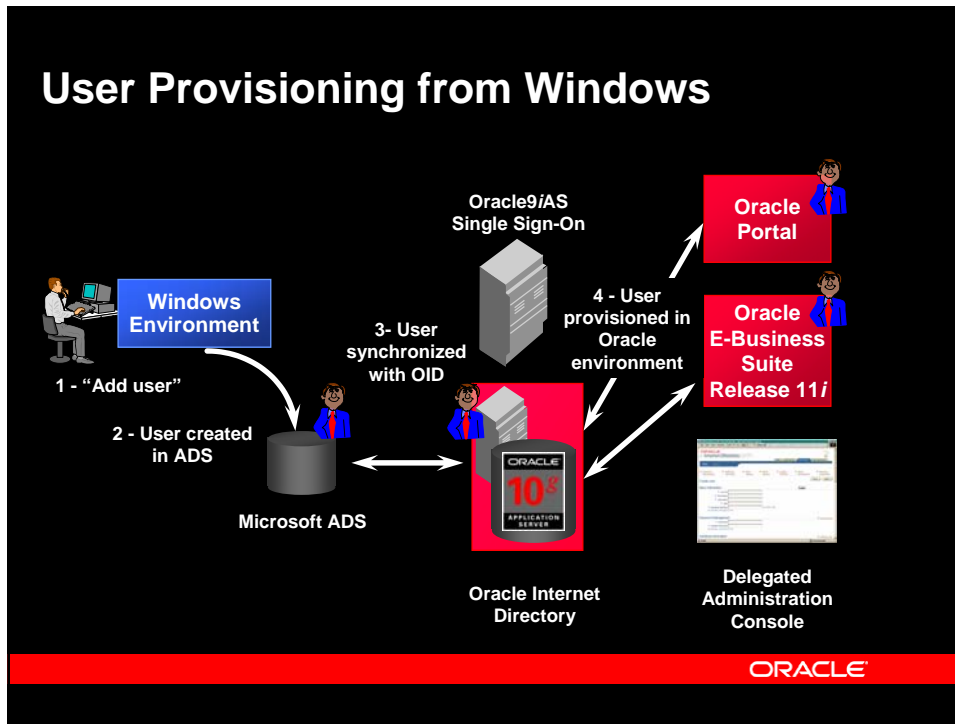
Integration Windows Active Directory

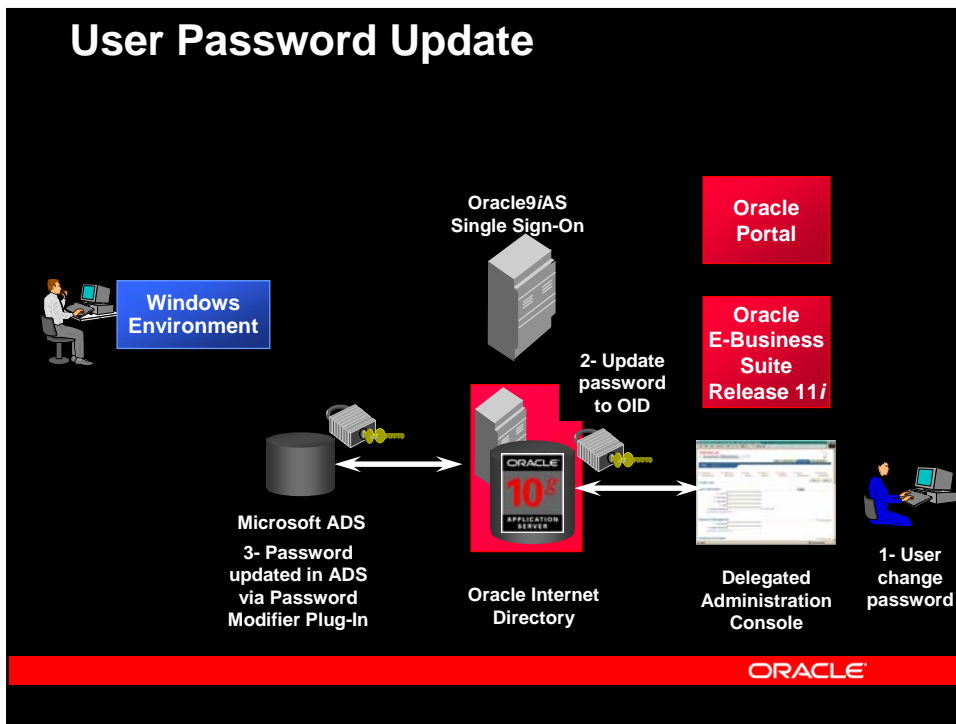
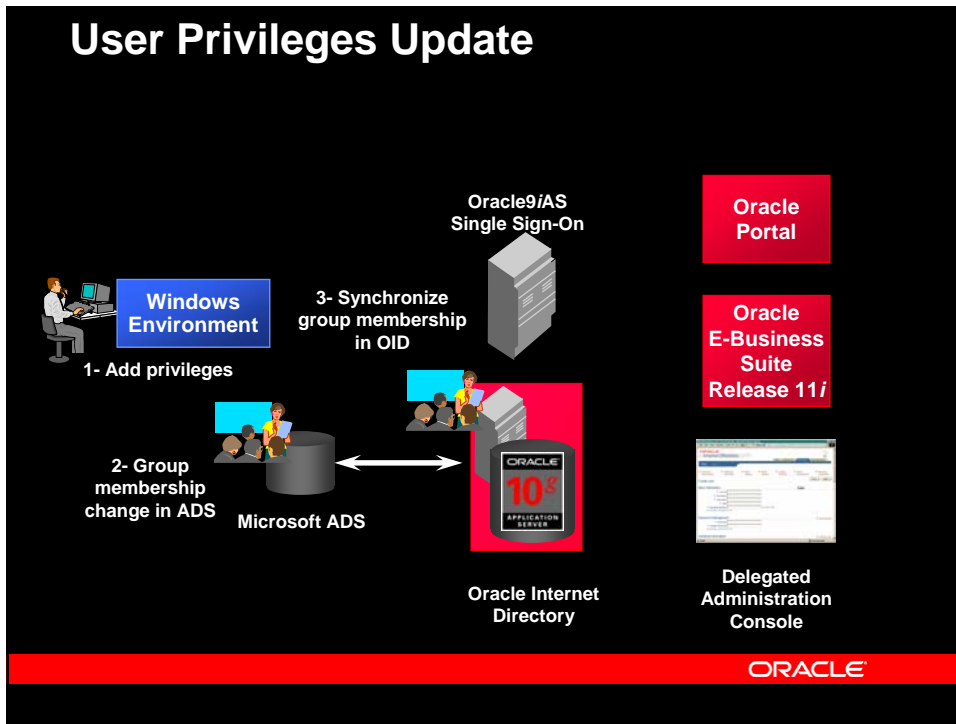
ORACLE

Windows Integration

- Windows Active Directory Connector für Oracle Internet Directory
 - Pre-packaged Lösung für Windows-Verzeichnisse
 - Bestandteil der Oracle Directory Integration Plattform
- Windows Native Authentication
 - “Automatic logon” zum Application Server basiert auf Windows logon (Kerberos)
 - Verbessert Windows Benutzer-Erfahrung
- Windows Authentifizierung und Password Plug-ins
 - “Referenziert” die Windows O/S Authentifizierung; keine Passwort Synchronisation erforderlich
 - Update des Windows Passworts durch Oracle Admin.-Werkzeuge

ORACLE

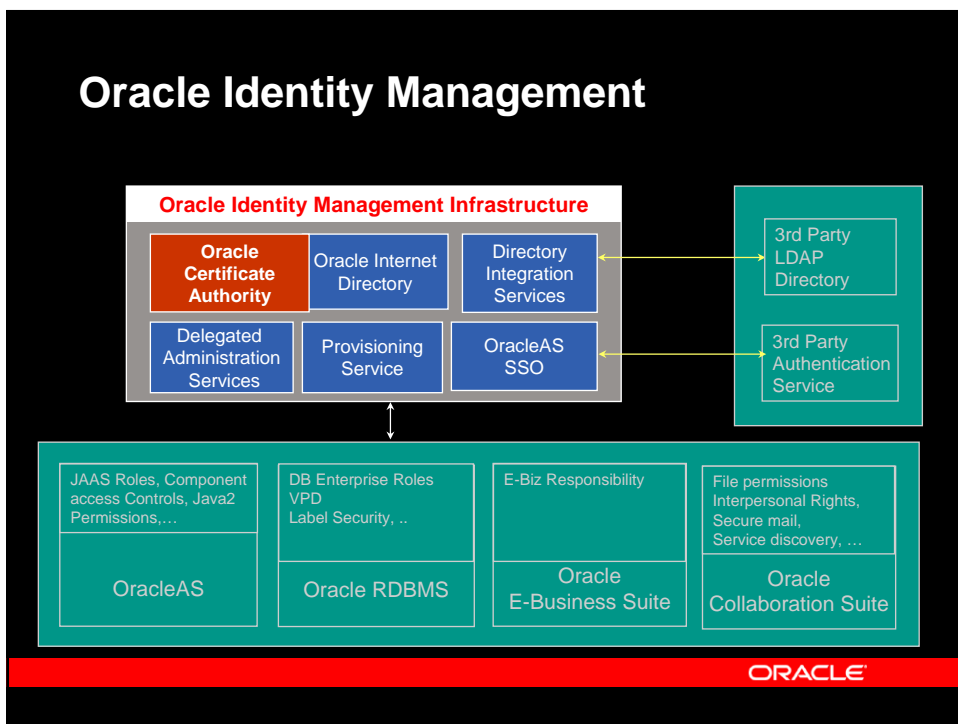




Demo

Authentifizierung Windows Active Directory

ORACLE



Oracle Certificate Authority

OracleAS 10^g (9.0.4)

- Out-of-the-box PKI Lösung
- Einfache Bereitstellung von X.509v3 Zertifikaten
- Ergänzt die Oracle PKI Story
- Nahtlose Integration mit OAS 10^g SSO Server
- Einfache Installation
- Standardkonformität
- Hochverfügbarkeit und Skalierbarkeit mit OracleAS 10^g und Oracle Internet Directory

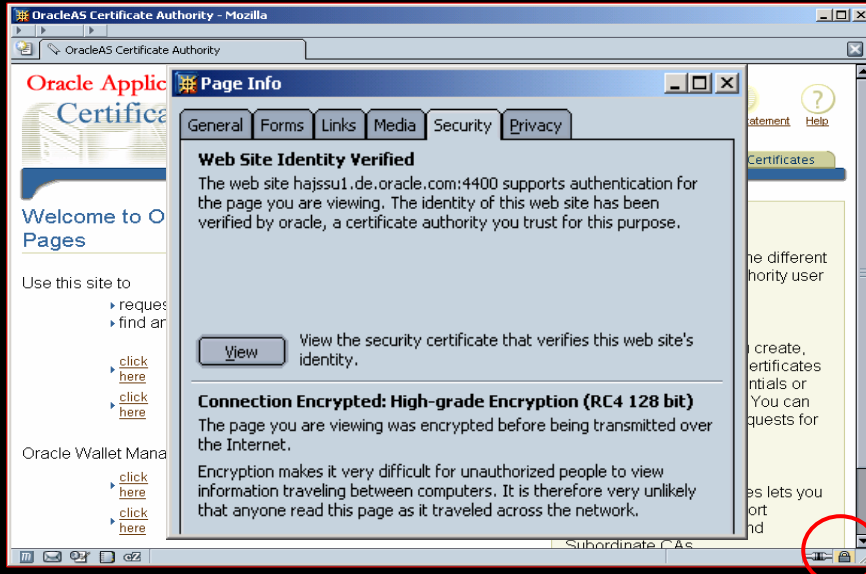
ORACLE

X.509 Zertifikate/ Oracle wallet

The screenshot displays two overlapping windows from the Oracle Certificate Authority. The 'Certificate Viewer' window shows details for a certificate issued to Olaf Stullich, including its validity period (03.04.2002 to 04.27.2003) and fingerprints. The 'Oracle Wallet Manager' window shows a tree view of certificates, with 'Certificate [Ready]' selected. A detailed view of the certificate is shown on the right, listing fields such as Subject Name (CN=heike juergense), Issuer Name (CN=olaf.stullich@ora), Version (X509v3), Serial Number (0x0B), Expiration Date (April 2, 2004), Key Size (1024), Key Type (RSA), Key Usage (SSL, MIME ENCRYP), and fingerprints (MD5: D9:A6:3F:FB:73:80:A...; SHA1: 4A:D6:29:41:D6:49:0...).

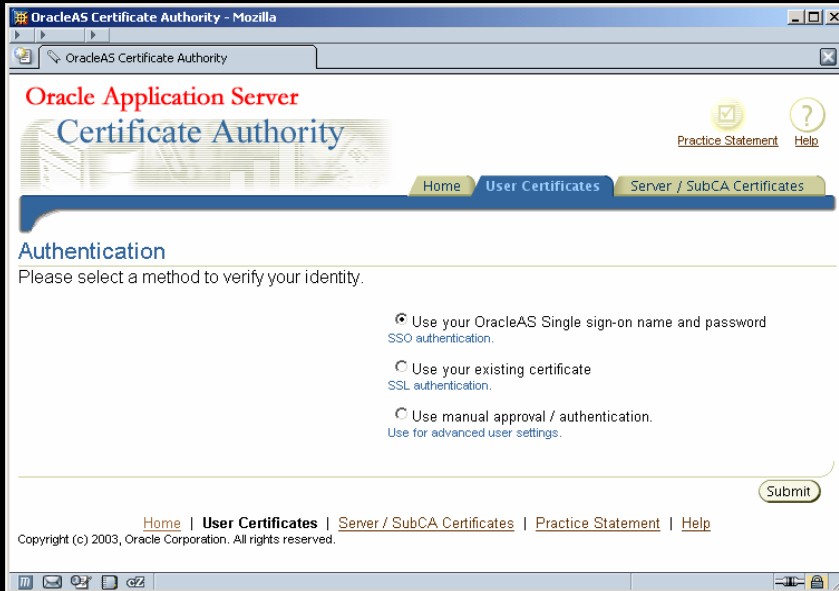
ORACLE

OracleAS 10g Oracle Certificate Authority



ORACLE

Oracle CA User Interface



ORACLE

Anwender Zertifikate (manuell) 1

The screenshot shows the Oracle Application Server Certificate Authority interface. The page title is "Oracle Application Server Certificate Authority". The navigation menu includes "Home", "User Certificates", and "Server / SubCA Certificates". The main content area is titled "User Certificates - Manual Authentication" and contains a search form with fields for "Certificate" and "ID / Serial No.", a "Go" button, and a "Request a Certificate" button. Below the search form is a table with columns: "Select", "Serial Number", "User DN", "Not Valid Before", "Not Valid After", "Status", "Usage", and "Revocation Reason". The table currently displays "No certificates retrieved." There are also buttons for "Download CA Certificate", "Download CRL", and "Change Authentication".

ORACLE

Benutzer Zertifikat (manuell) 2

The screenshot shows the Oracle Application Server Certificate Authority interface for a certificate request form. The page title is "Oracle Application Server Certificate Authority". The navigation menu includes "Home", "User Certificates", and "Server / SubCA Certificates". The main content area is titled "Certificate Request Form - Manual Authentication" and contains a form for entering DN information. The form fields are: "Common Name" (olaf.stullich), "E-Mail Address" (olaf.stullich@oracle.com), "Organizational Unit" (BU Datenbank), "Organization" (Sales), and "City/Locality" (Hannover). There is also an "Advanced DN" link.

ORACLE

Benutzer Zertifikat (manuell) 3

The screenshot shows the Oracle Application Server Certificate Authority interface in a Mozilla browser window. The page title is "Oracle Application Server Certificate Authority". The navigation menu includes "Home", "User Certificates", and "Server / SubCA Certificates". A central message box with an information icon states: "Your certificate request is accepted. Administrator will contact you for certificate issuance. Your request ID is '15'. Please use this request ID for future reference." Below the message is an "OK" button. The footer contains copyright information: "Copyright (c) 2003, Oracle Corporation. All rights reserved."

ORACLE

User Zertifikat (Admin Sicht)

The screenshot shows the Oracle Application Server Certificate Authority admin interface in a Mozilla browser window. The page title is "Oracle Application Server Certificate Authority - Certificate Management". The navigation menu includes "Home", "Certificate Management", "Configuration Management", and "View Logs". A search bar is present with "Certificate Request" selected and "All Pending Requests" in a dropdown. Below the search bar is a table titled "Certificate Management" with the following data:

Select	Request ID	User DN	Request Type	Request Date	Status	Serial Number
<input type="radio"/>	15	CN=olaf.stullich,Email=olaf.stullich@oracle.com,OU=BU Database,O=Sales,L=Hannover,C=DE	client	February 26, 2004	Pending	

Below the table is an "Update Certificate Revocation List(CRL)" button. The footer contains copyright information: "Copyright (c) 2003, Oracle Corporation. All rights reserved."

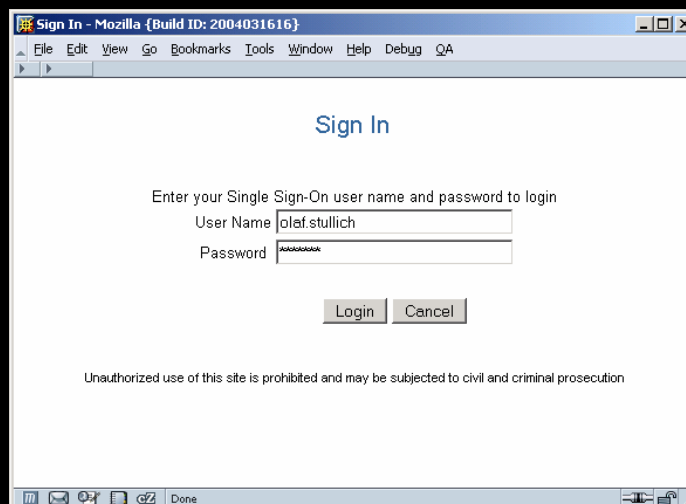
ORACLE

Oracle CA User Interface



ORACLE

Benutzeranmeldung SSO



ORACLE

Request User Certificate

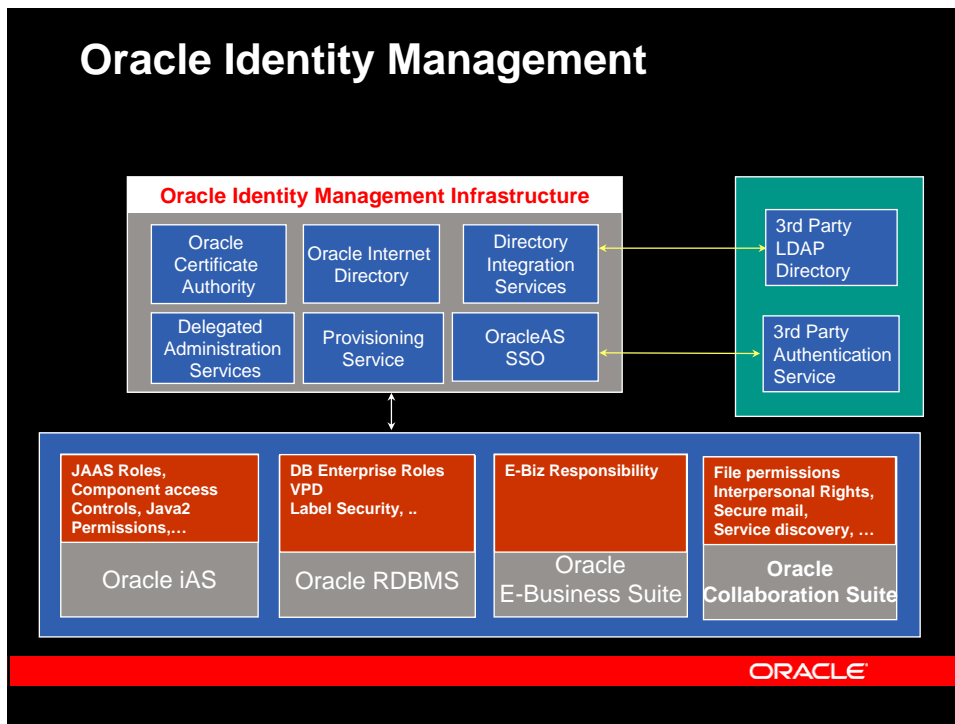


The screenshot shows a web browser window titled "Oracle Certificate Authority-Certificate Request Form - SSO Authentication - Mozilla". The page header includes the Oracle9iAS logo and navigation links for "Practice Statement", "Help", and "Logout". Below the header, there are tabs for "Home", "User Certificates", and "Server / SubCA Certificates". The main content area is titled "Certificate Request Form - SSO Authentication" and includes the instruction: "Use this form to request a certificate for a SSO user." The form is divided into two sections: "DN Information" and "Certificate Information". In the "DN Information" section, the "User DN" field contains the text "cn=ostullic, cn=users, dc=de, dc=oracle, dc=com". In the "Certificate Information" section, the "Certificate Key Size" dropdown is set to "2048 (High Grade)" with a note: "Select the size of the certificate key to generate. The bigger the size, the greater the strength." The "Certificate Usage" dropdown is set to "SSL / Encryption". The Oracle logo is visible in the bottom right corner of the slide.

Oracle Identity Management – Vorteile

- Eine Unternehmensinfrastruktur, die die “unbreakable” Technologie von Oracle einsetzt
 - *Hochverfügbarkeit, Skalierbarkeit, Sicherheit, Performance*
- Vereinfacht die Verteilung aller Oracle Produkte
 - *AS, DB, OCS, eBiz*
- Zentraler Integrationspunkt für existierende Kunden Identity Management Lösungen
 - *Transparente 3rd party Integration von OIM basierten Produkten*
- Eine offene, standard-basierte Infrastruktur
 - *anpassbar an unterschiedliche Partnerlösungen und Kundenbedürfnisse*

ORACLE



Informationen: Olaf.Stullich@oracle.com

- <http://www.oracleworld2003.com/scps/controller/catalog>
 - Solution Areas
 - Security and Identity Management (23)
- <http://otn.oracle.com/deploy/security/index.html>

