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 Veranwortlichkeiten delegieren
- Administratoren Anwendungen leicht & sicher verteilen
- Anwender selbständig Passwörter und Preferenzen ändern können
- Benutzer einen Single Sign-On Zugang haben

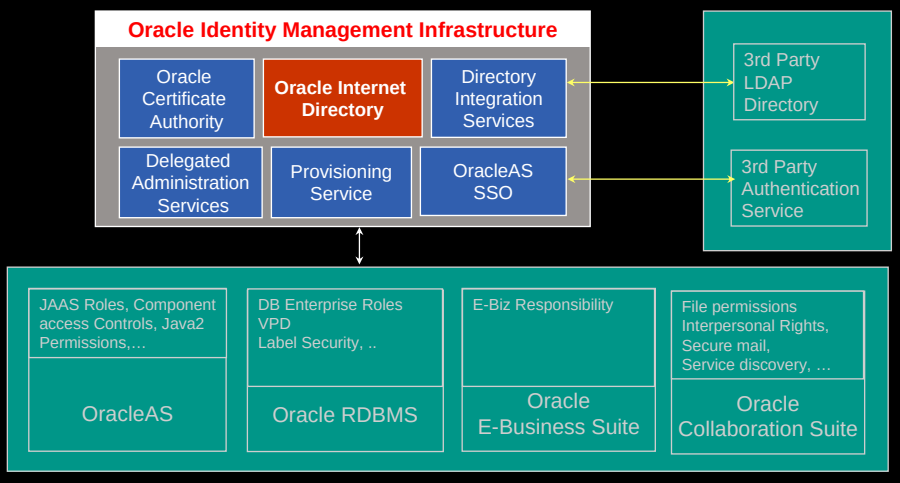
ORACLE

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

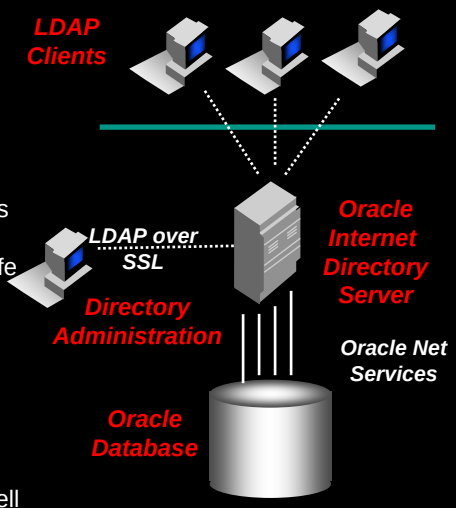
Was sind Verzeichnisdienste ?

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

ORACLE

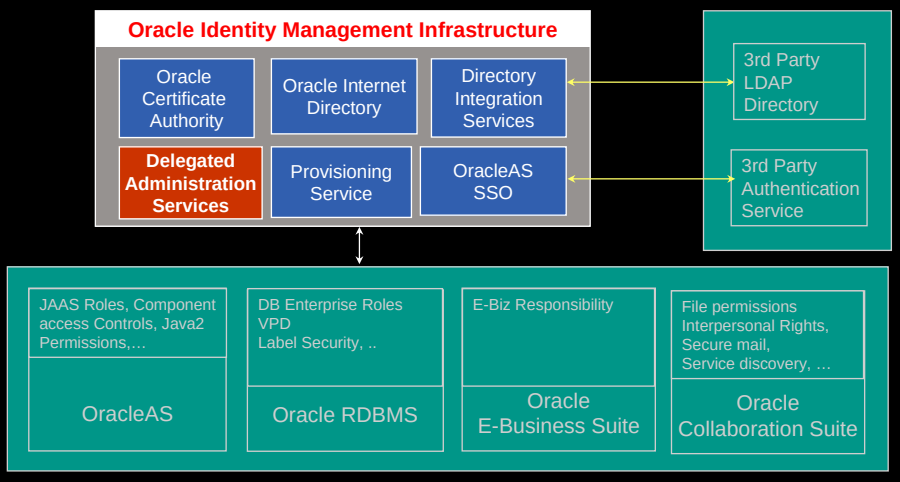
Oracle Internet Directory

- 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

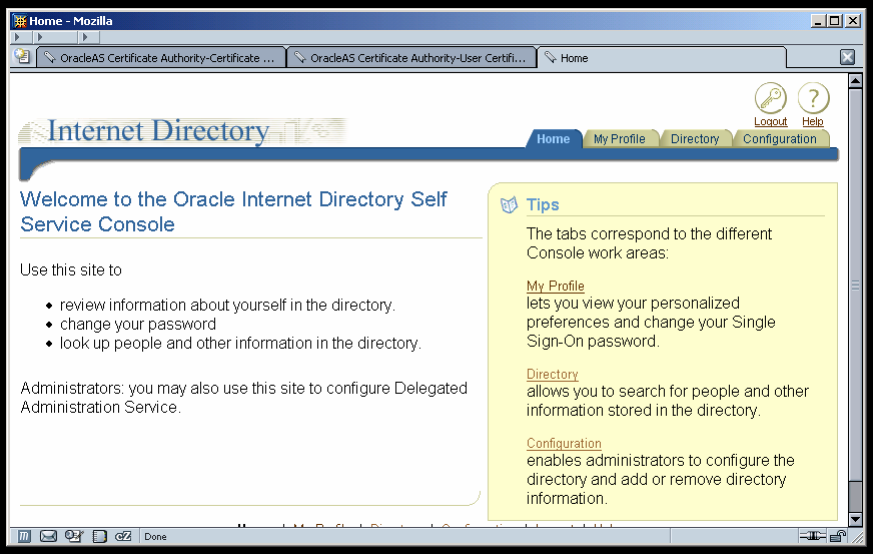
Oracle Identity Management



Delegated Administration Services

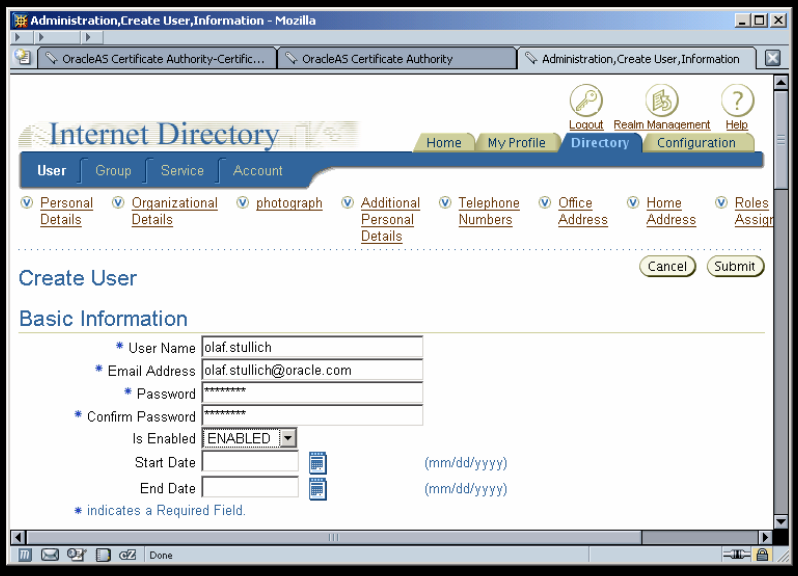
- Einheitliche Schnittstelle zur Directory Datenverwaltung
  - Administrator: unterstützt Benutzer und anwendungsspezifische Berechtigungsverwaltung
  - Endanwender: ändern von Passwörtern, Preferenzen, Profilen etc.

Delegated Administration Service



ORACLE

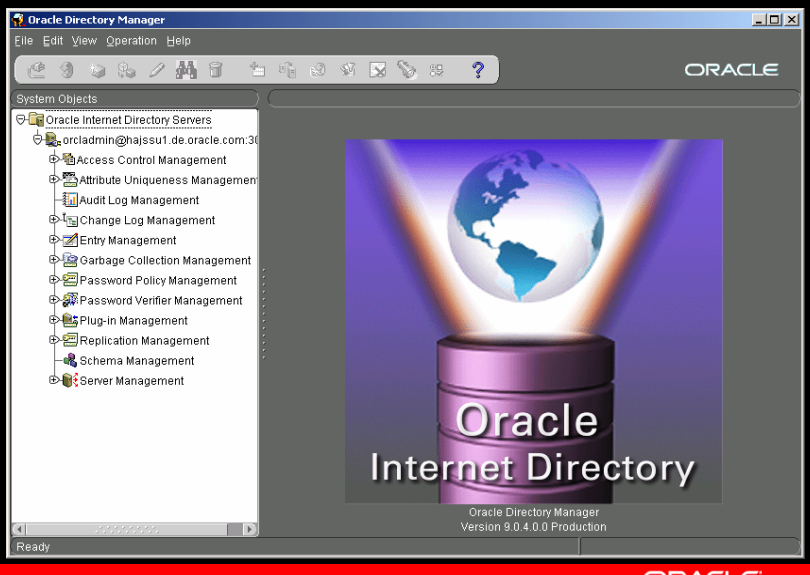
Benutzer anlegen



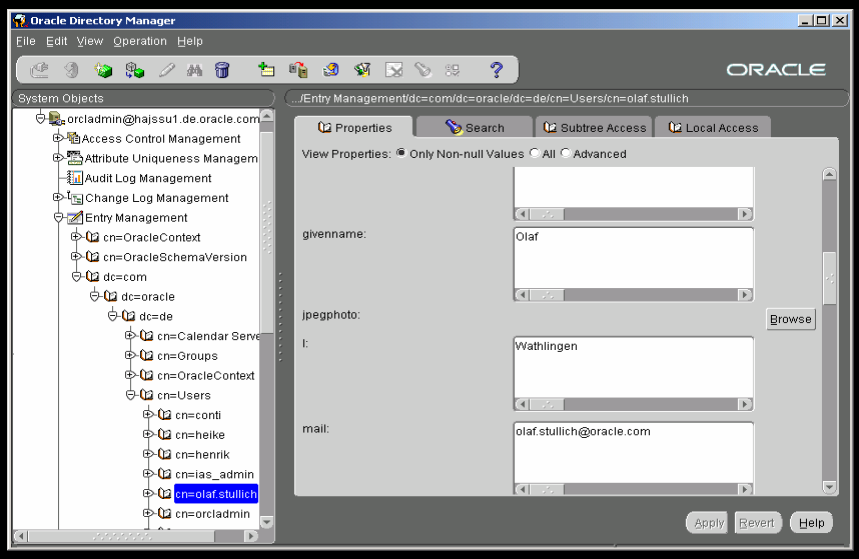
ORACLE

Benutzerprofil

OID Admin Console

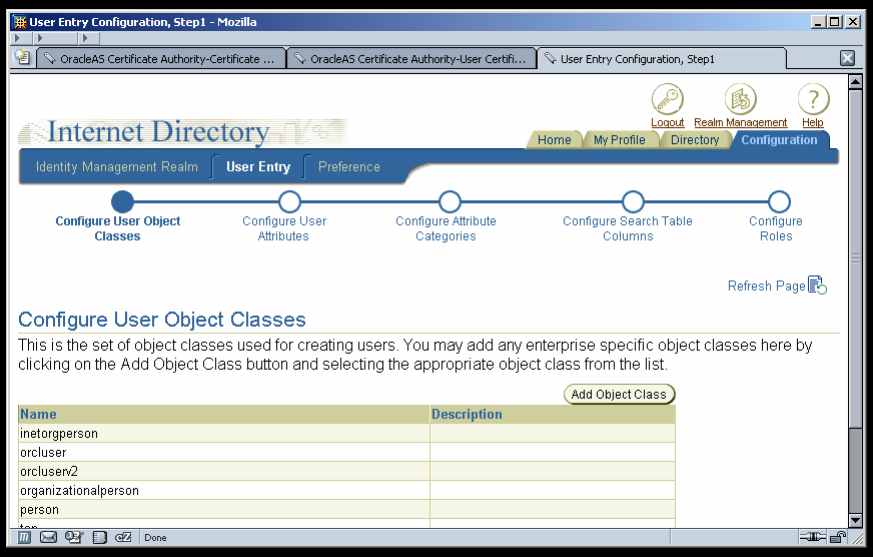


OID Admin Console



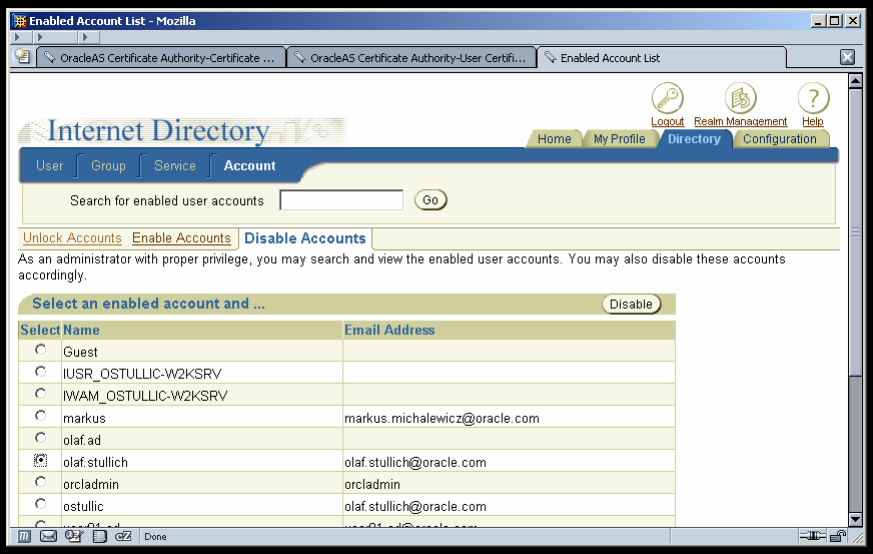
ORACLE

Benutzer Einstellungen



ORACLE

Disable user accounts

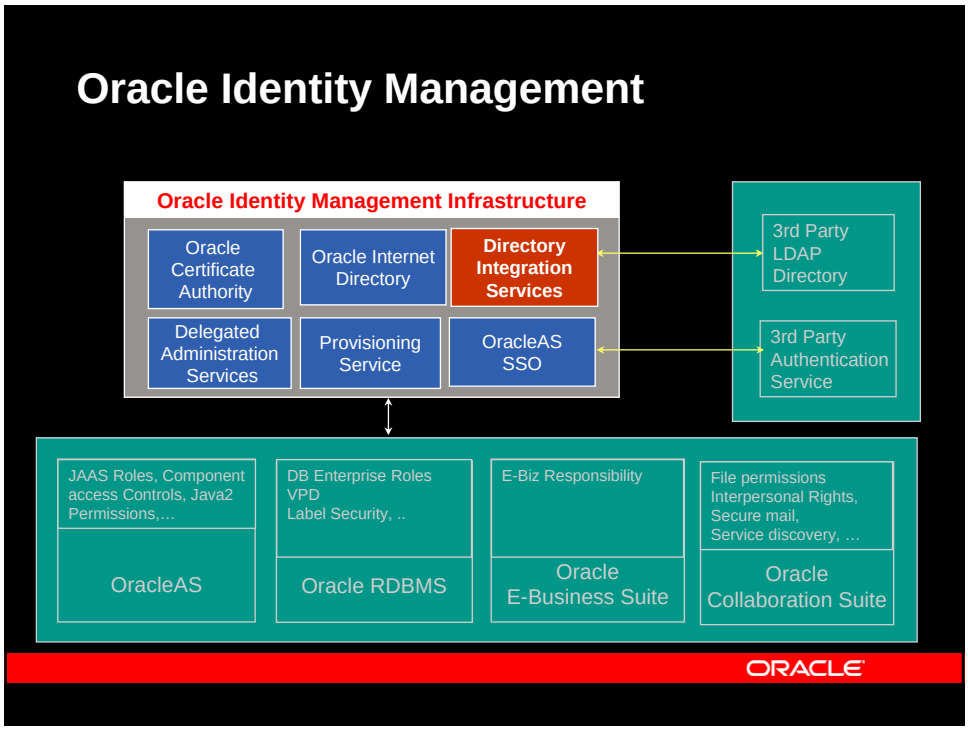


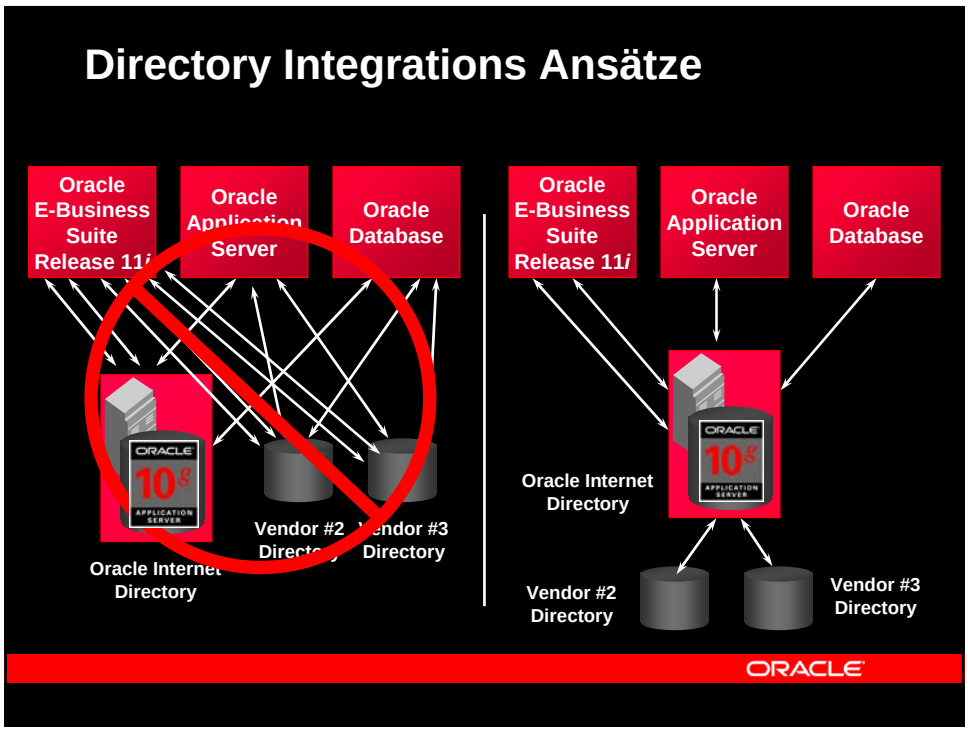
ORACLE

Demo

Delegated Adminstration Service

ORACLE


Oracle Identity Management
Oracle Identity Management Infrastructure
Oracle Certificate Authority
Oracle Internet Directory
Directory Integration Services
Delegated Administration Services
Provisioning Service
OracleAS SSO
3rd Party LDAP Directory
3rd Party Authentication Service
JAAS Roles, Component access Controls, Java2 Permissions,…
OracleAS
DB Enterprise Roles
VPD
Label Security, ..
Oracle RDBMS
E-Biz Responsibility
Oracle E-Business Suite
File permissions
Interpersonal Rights,
Secure mail,
Service discovery, …
Oracle Collaboration Suite
ORACLE


Directory Integrations Ansätze
Oracle E-Business Suite Release 11i
Oracle Application Server
Oracle Database
Oracle Internet Directory
Vendor #2 Directory
Vendor #3 Directory
Oracle E-Business Suite Release 11i
Oracle Application Server
Oracle Database
Oracle Internet Directory
Vendor #2 Directory
Vendor #3 Directory
ORACLE

mySap.com Zertifizierung

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

CERTIFICATE

Interface Software for mySAP.com

SAP AG hereby confirms that the interface software for the product

Oracle Internet Directory (OID) 9.2

of the company

Oracle Corporation

has been certified for the component SAP Web Application Server 6.20 and SAP LDAP Connector 2.1.

This certificate confirms the existence of product functionality in accordance with SAP's certification procedure. It does not guarantee that the product is error-free.

The certification test is documented in report: 1400/14755/468716/wdf dating May 23, 2002.

The test has been performed using an SAP Web Application Server 6.20 System.

Vendor Hardware: PC-Pentium
Operating system: Windows 2000

This configuration meets the requirements for connecting Oracle Internet Directory (OID) to the mySAP.com platform.

BC-LDAP-USR 6.20 and SAP LDAP Connector 2.1- Directory Interface for User Management via LDAP
Oracle Internet Directory (OID) for the mySAP.com platform

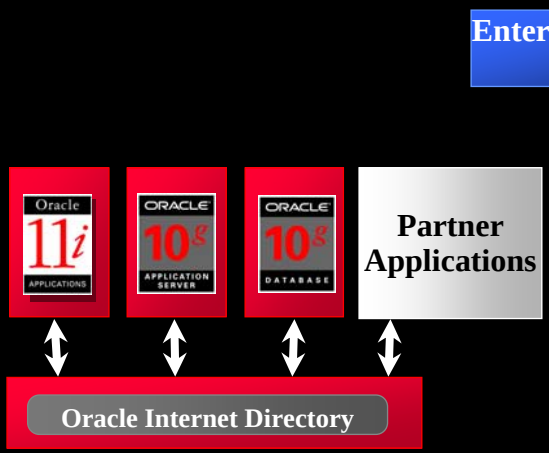
Certified functions
Automatic schema extensions using LDIF file
Mapping using transaction LDAPMAP
Synchronization using transaction RSLDAPSYNC_USR

Walldorf, October 02, 2002

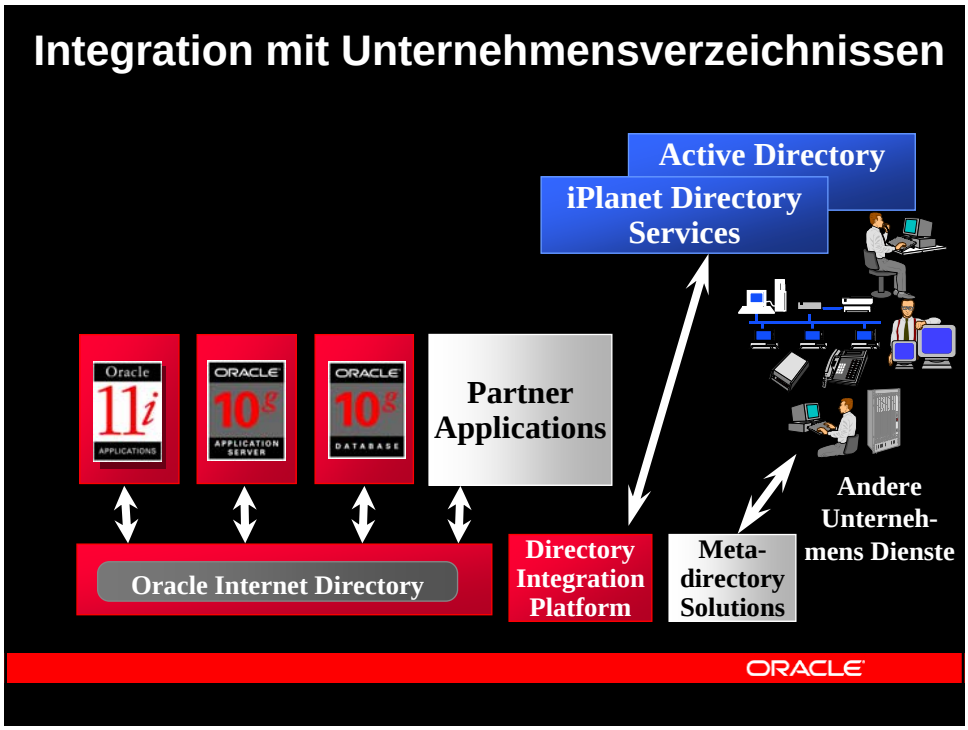
Director Integration & Certification Center
SAP AG

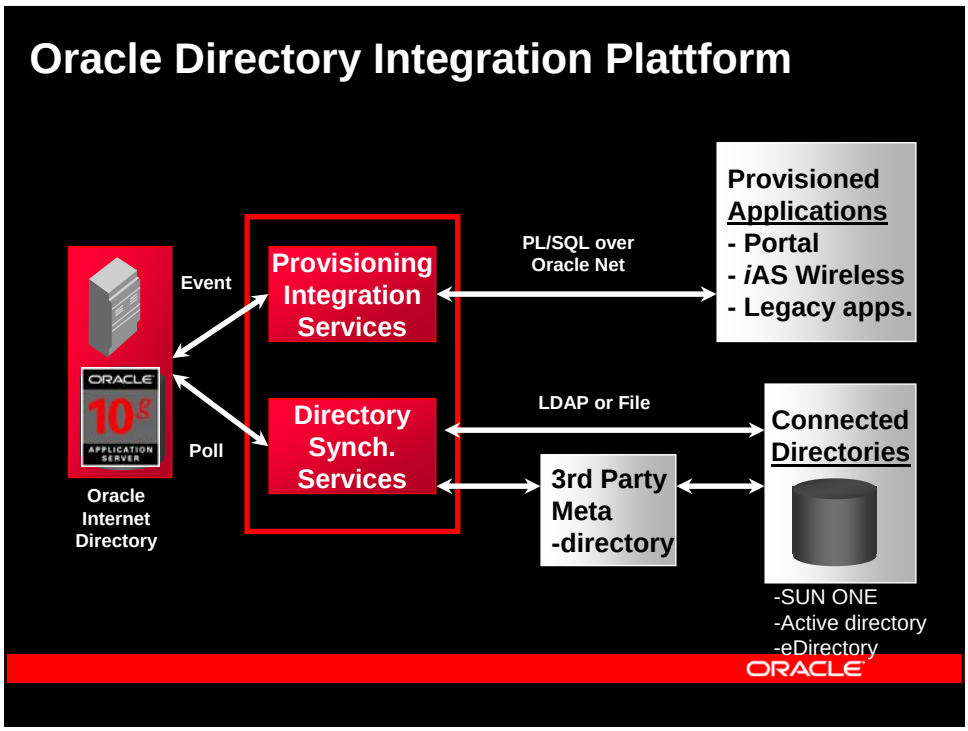
ORACLE

Integration mit Unternehmensverzeichnissen

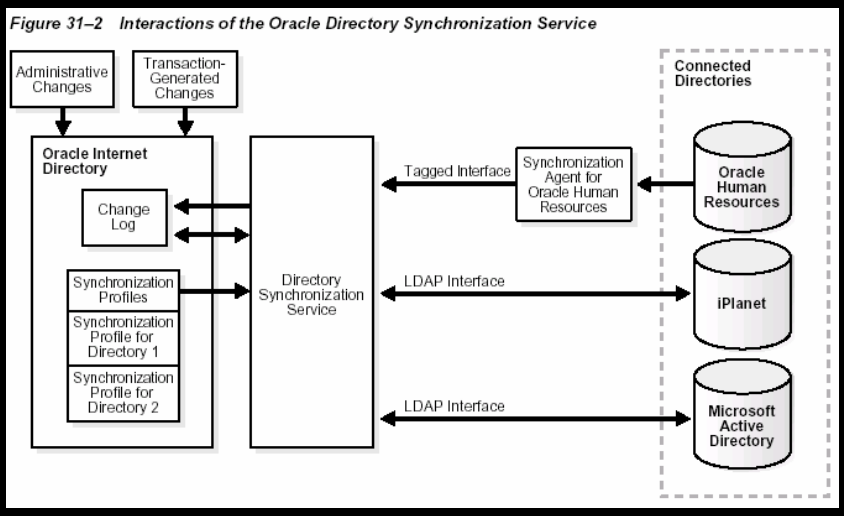


ORACLE


Integration mit Unternehmensverzeichnissen
Active Directory
iPlanet Directory Services
Partner Applications
Oracle Internet Directory
Directory Integration Platform
Meta-directory Solutions
Andere Unterneh-mens Dienste
ORACLE


Oracle Directory Integration Plattform
Event
Poll
Oracle Internet Directory
Provisioning Integration Services
Directory Synch. Services
PL/SQL over Oracle Net
LDAP or File
Provisioned Applications
- Portal
- iAS Wireless
- Legacy apps.
3rd Party Meta -directory
Connected Directories
-SUN ONE
-Active directory
-eDirectory
ORACLE

Directory Synchronisation



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

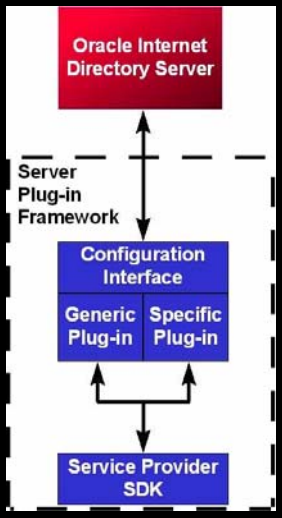
Directory Synchronization Profiles

- 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 Syschronisation Profile ab

ORACLE

Oracle Internet Directory Plug-In Framework

- Neue Funktionalität mit Oracle9*i* Application Server R2
- Plug-in`s sind PL/SQL packages
- Erlaubt Aufruf Benutzer-definierter Operationen
- Aufruf bei LDAP Kommando Ausführung
  - ldapbind, ldapadd, ldapmodify, ldapcompare, ldapsearch, ldapdelete



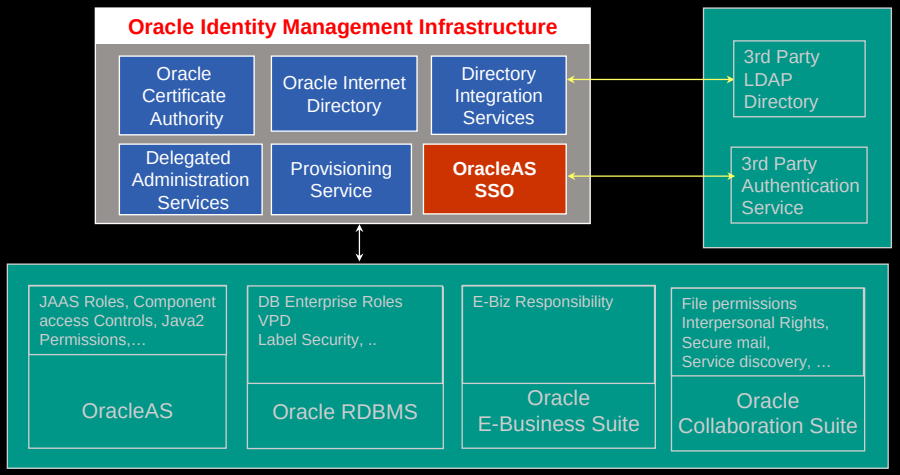
ORACLE

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

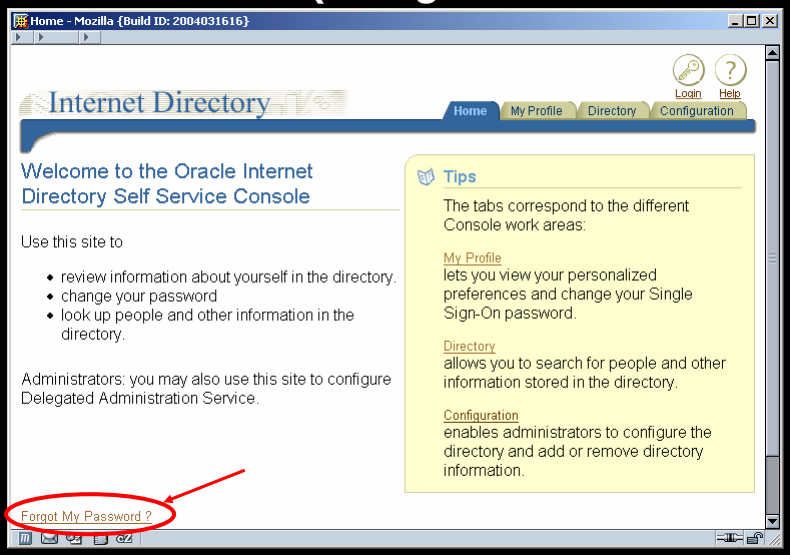
Sicherheit aller Applikationen

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

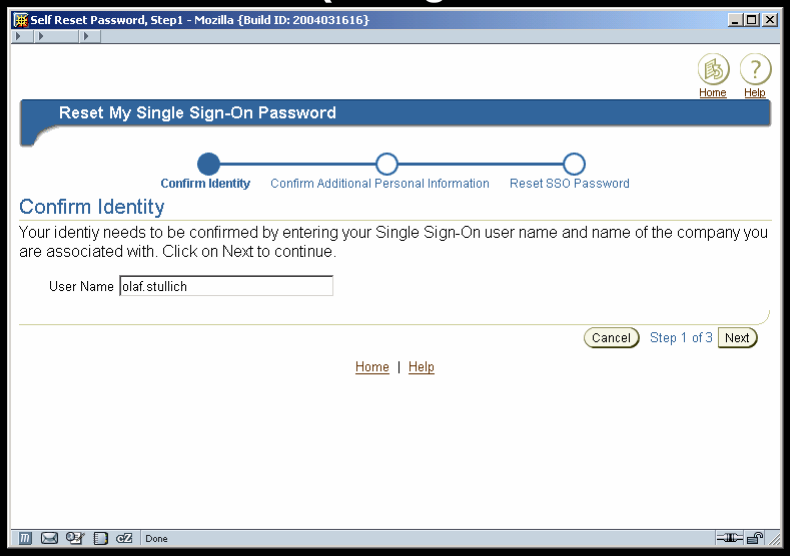
ORACLE

Password Reset 1 (Delegated Admin Service)

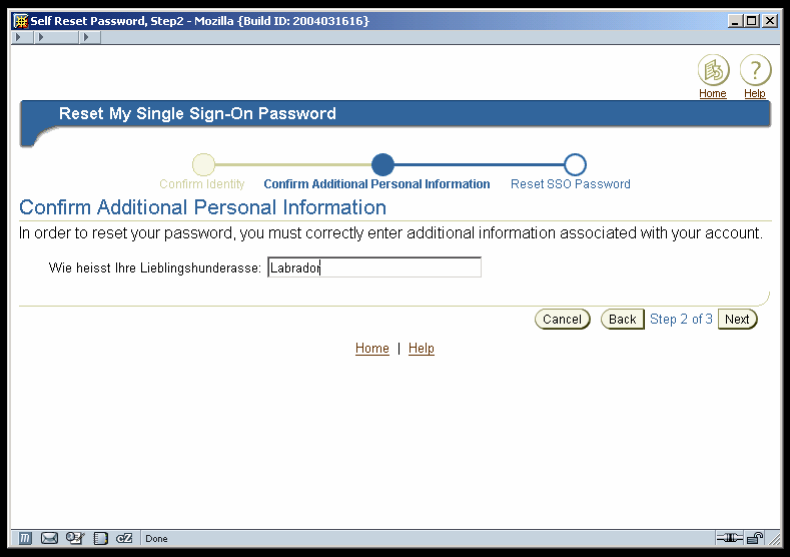


ORACLE

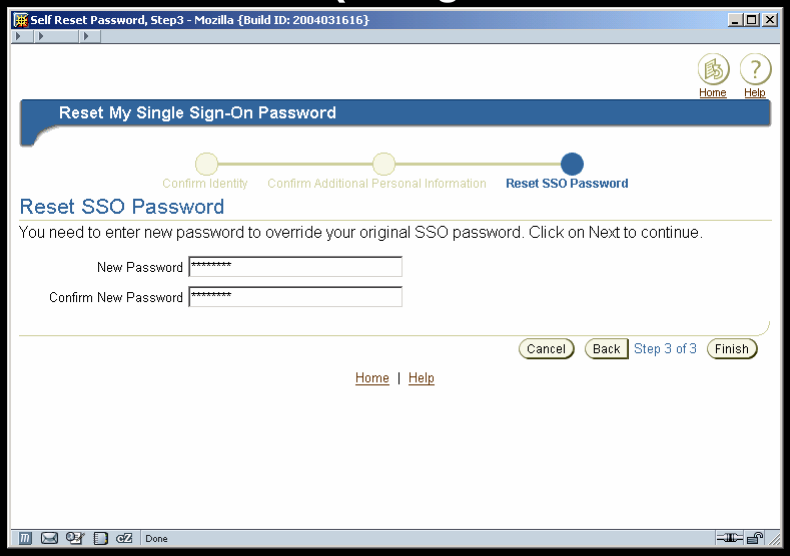
Password Reset 2 (Delegated Admin Service)



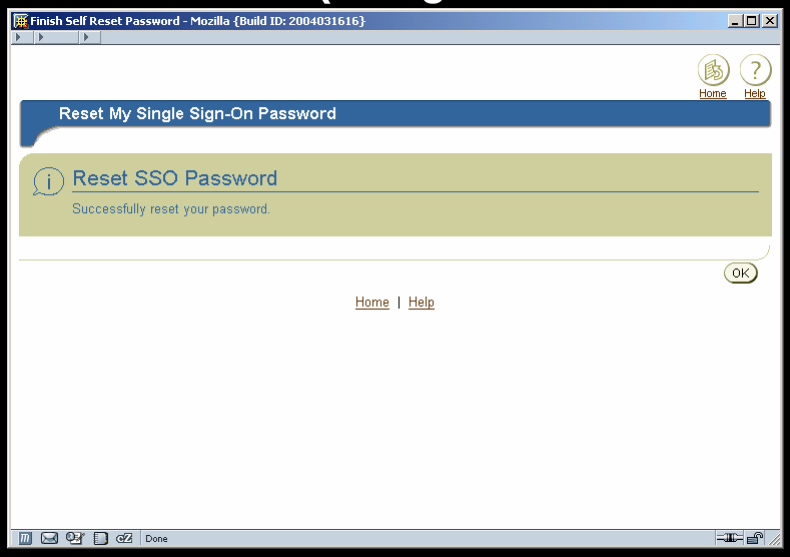
Passwort Reset 3 (Delegated Admin Service)



Password Reset 3 (Delegated Admin Service)



Passwort Reset 4 (Delegated Admin Service)



Demo

Delegated Adminstration Service

Password Reset

ORACLE

Definitionen

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

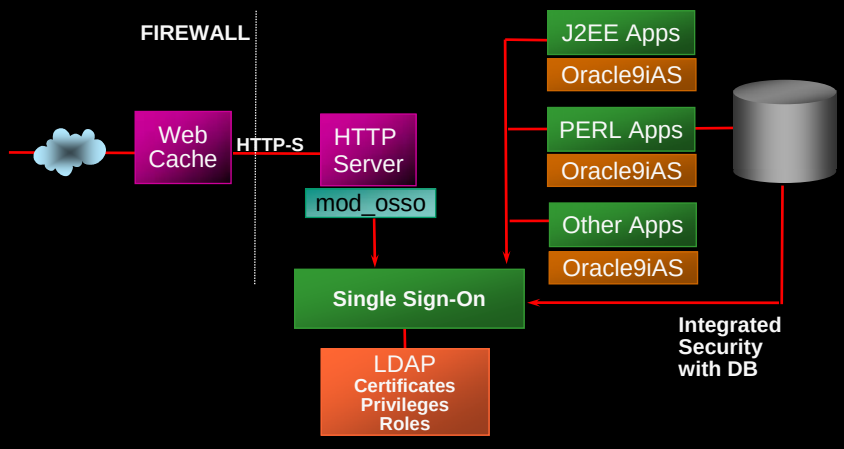
ORACLE

Oracle SSO Server

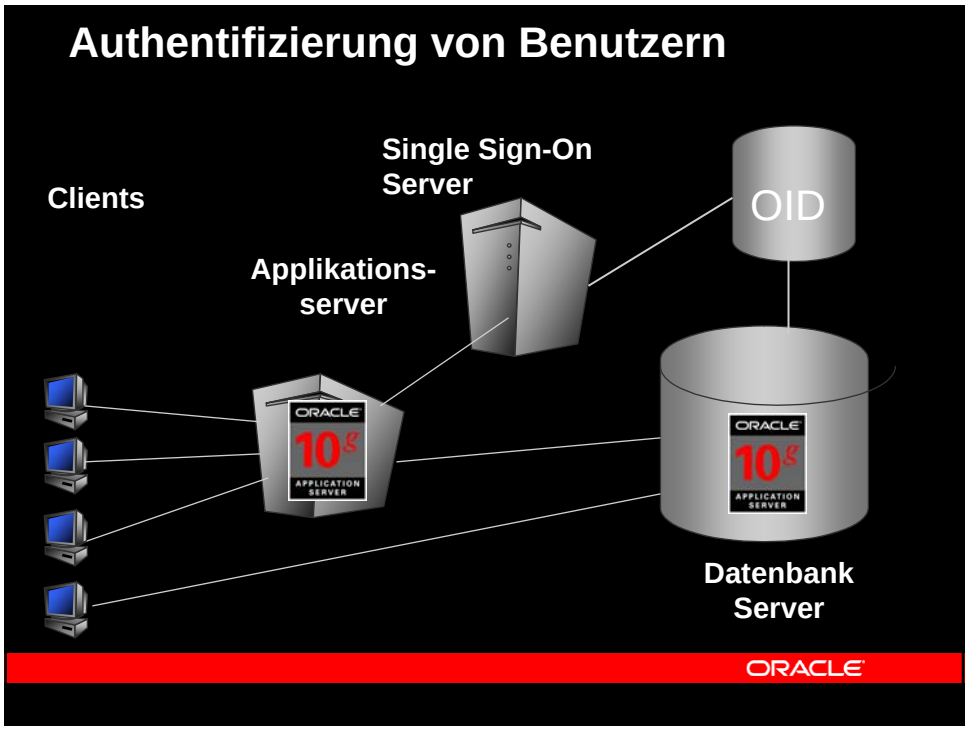
- Kernkomponente der Oracle's Web SSO Technologie
- Authentifiziert Benutzer und reicht deren Identität sicher an Partner-Anwendungen weiter
- Fordert den Benutzer zur Eingabe eines Namens und Passwortes auf:
  - beim erstmaligen Systemzugriff innerhalb einer vorgegebenen Zeit
  - verifiziert das Passwort

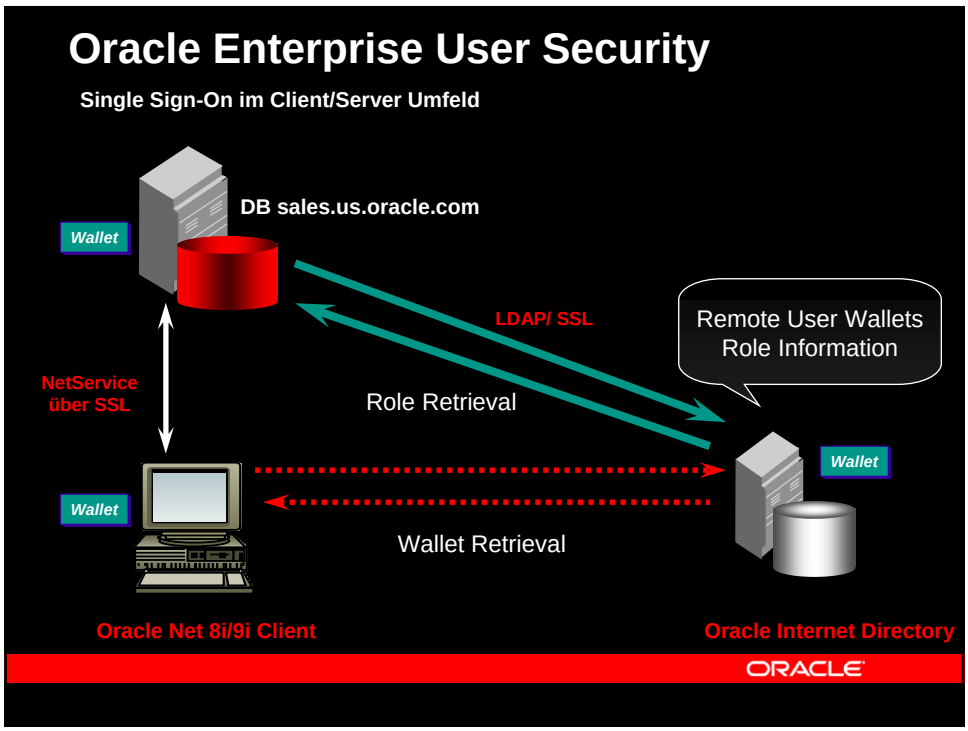
ORACLE

Architektur

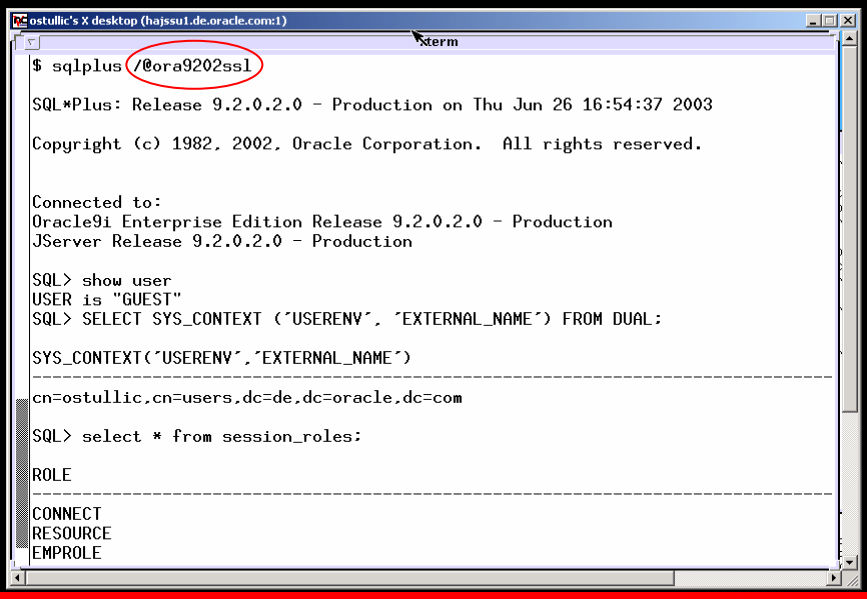


ORACLE

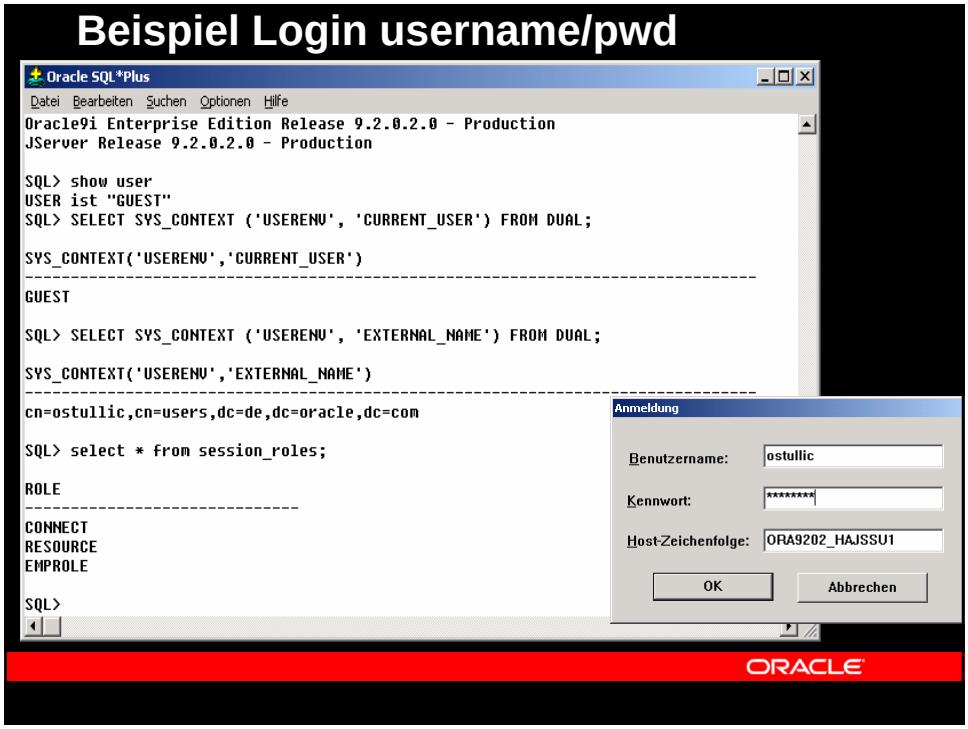

Authentifizierung von Benutzern
Clients
Single Sign-On Server
OID
Applikations-server
ORACLE
10g
APPLICATION SERVER
Datenbank Server
ORACLE


Oracle Enterprise User Security
Single Sign-On im Client/Server Umfeld
DB sales.us.oracle.com
Wallet
LDAP/ SSL
Remote User Wallets
Role Information
NetService über SSL
Role Retrieval
Wallet
Wallet
Wallet Retrieval
Oracle Net 8i/9i Client
Oracle Internet Directory
ORACLE

Bsp SSL based authentication



Beispiel Login username/pwd



Beispiel

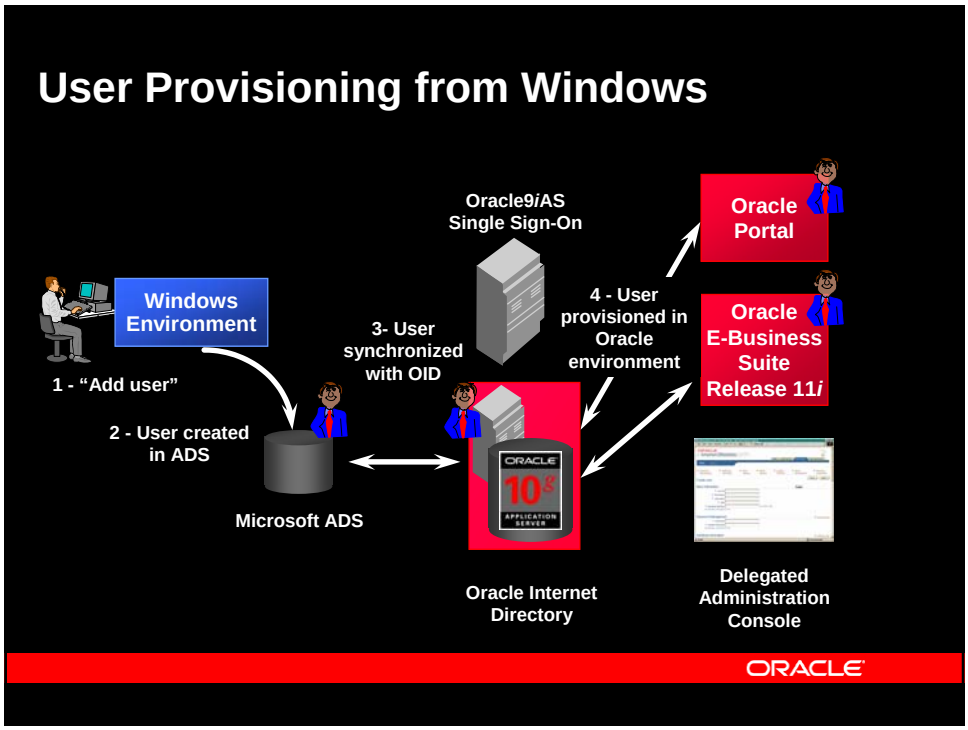
Integration Windows Active Directoy

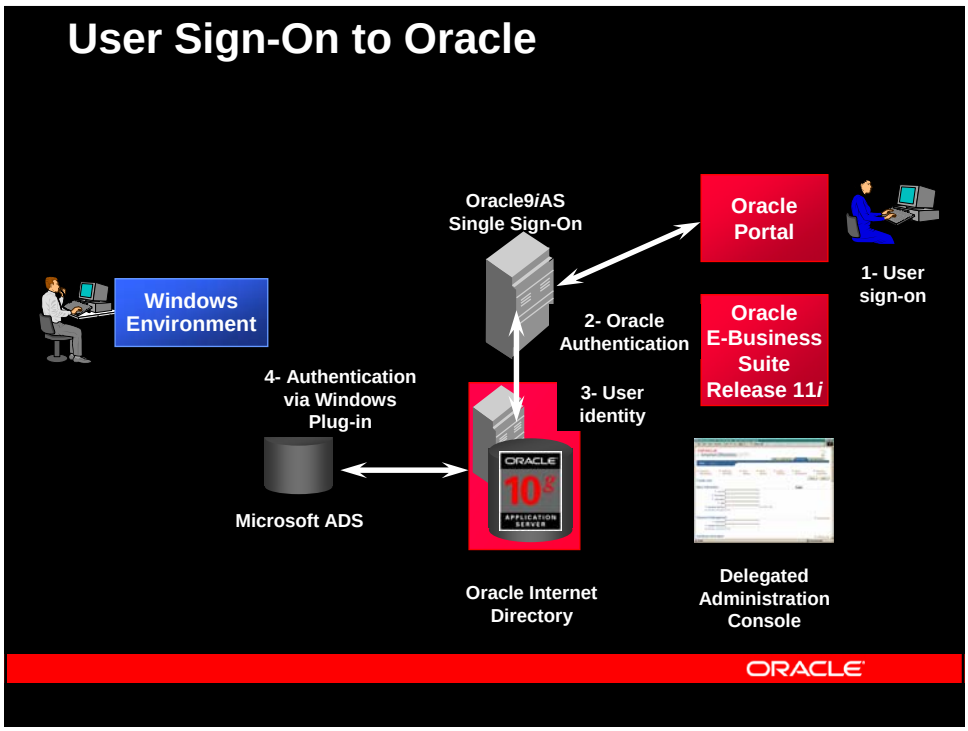
ORACLE

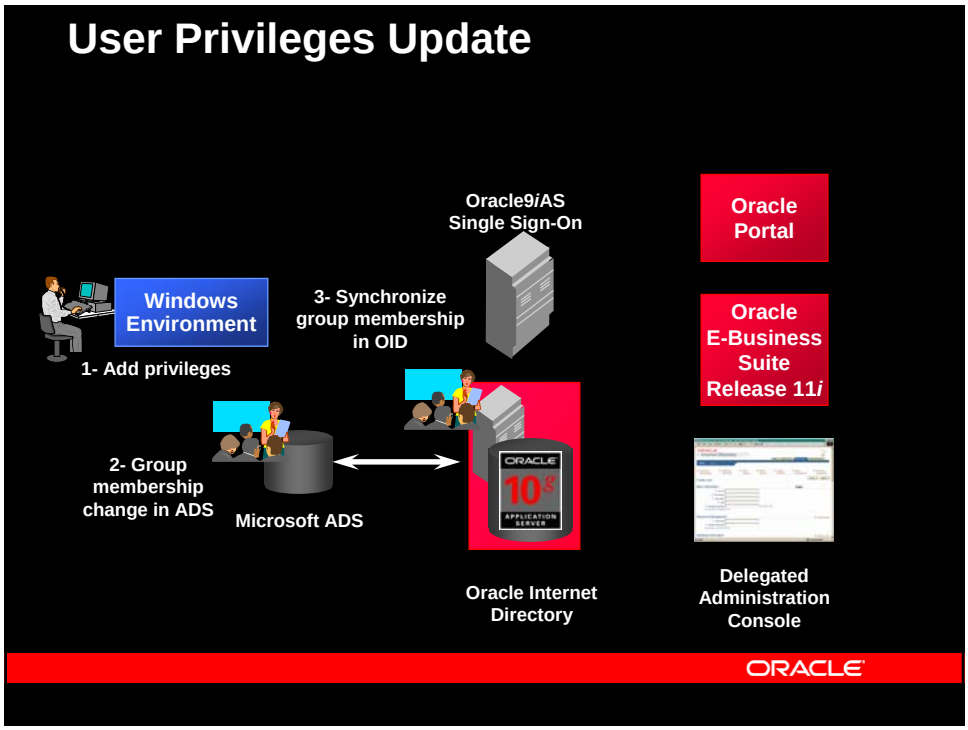
Windows Integration

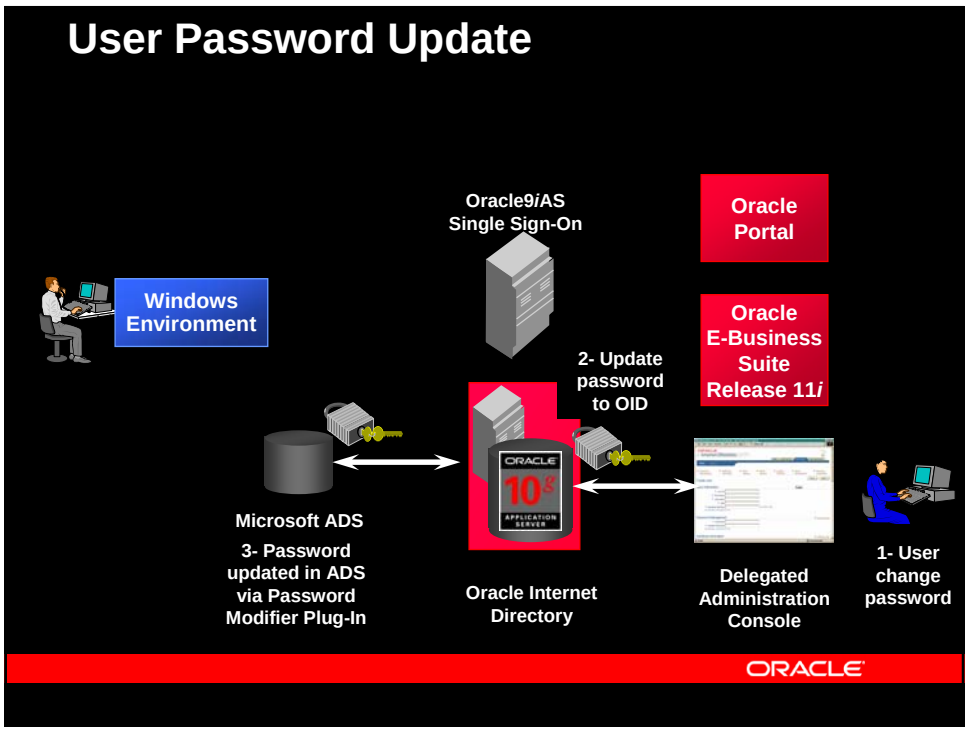
- Windows Active Directory Connector für Oracle Internet Directory
  - Pre-packaged Lösung für Windows-Verzeichnisse
  - Bestandteil der Oracle Directory Integration Plattform
- Windows Native Authentication
  - “Automatic logon” zum Application Server basiert auf Windows logon (Kerberos)
  - Verbessert 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


User Provisioning from Windows
Oracle9iAS Single Sign-On
Oracle Portal
Windows Environment
3- User synchronized with OID
4 - User provisioned in Oracle environment
Oracle E-Business Suite Release 11i
1 - "Add user"
2 - User created in ADS
Microsoft ADS
Oracle Internet Directory
Delegated Administration Console
ORACLE


User Sign-On to Oracle
Oracle9iAS Single Sign-On
Oracle Portal
1- User sign-on
Windows Environment
2- Oracle Authentication
Oracle E-Business Suite Release 11i
4- Authentication via Windows Plug-in
3- User identity
Microsoft ADS
Oracle Internet Directory
Delegated Administration Console
ORACLE


User Privileges Update
Oracle9iAS
Single Sign-On
Oracle
Portal
Windows
Environment
3- Synchronize
group membership
in OID
Oracle
E-Business
Suite
Release 11i
1- Add privileges
2- Group
membership
change in ADS
Microsoft ADS
Oracle Internet
Directory
Delegated
Administration
Console
ORACLE

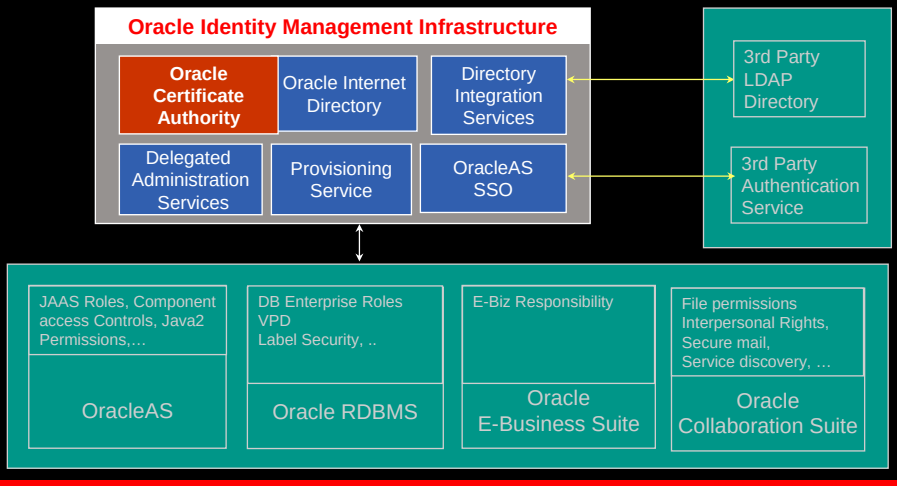

User Password Update
Oracle9iAS
Single Sign-On
Oracle
Portal
Windows
Environment
2- Update
password
to OID
Oracle
E-Business
Suite
Release 11i
Microsoft ADS
3- Password
updated in ADS
via Password
Modifier Plug-In
Oracle Internet
Directory
Delegated
Administration
Console
1- User
change
password
ORACLE

Demo

Authentifzierung
Windows Active Directory

ORACLE

Oracle Identity Management



ORACLE

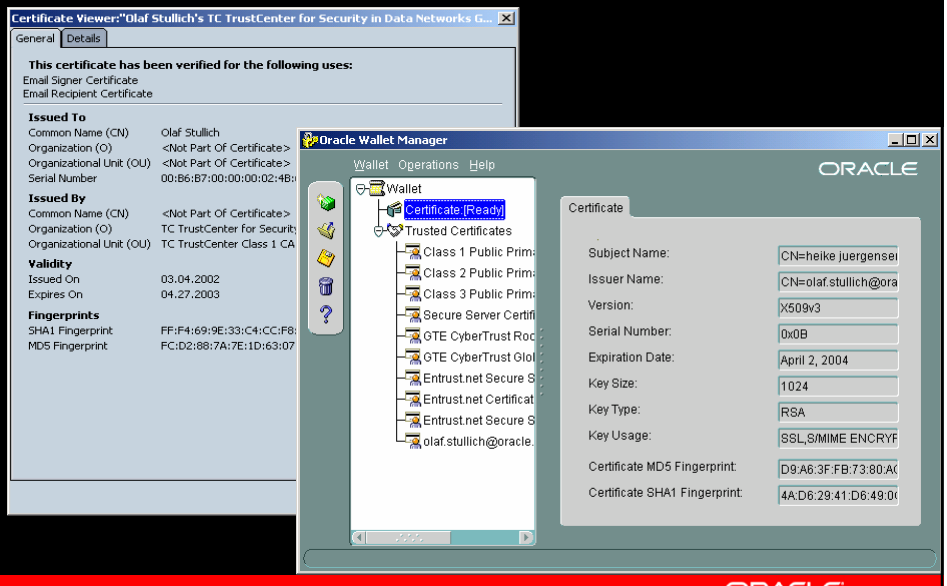
Oracle Certificate Authority

OracleAS 10g (9.0.4)

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

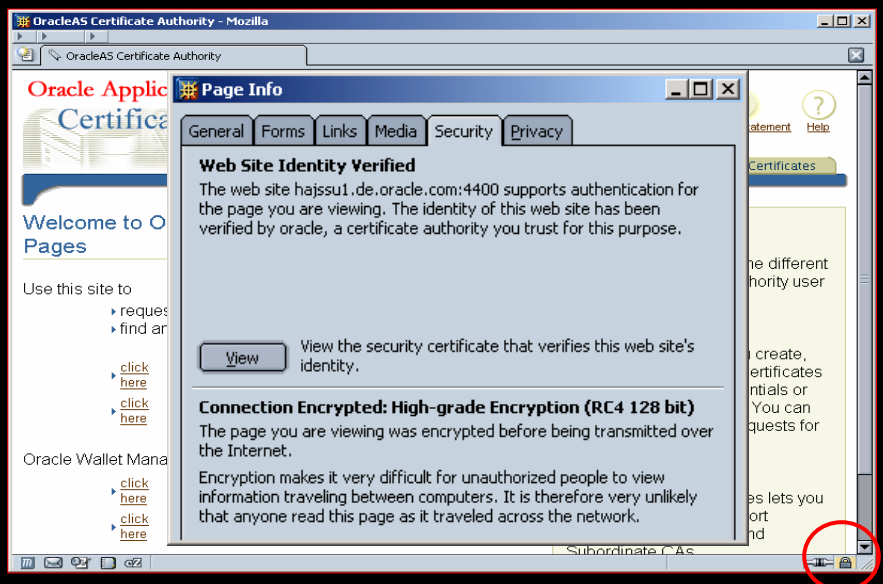
ORACLE

X.509 Zertifikate/ Oracle wallet

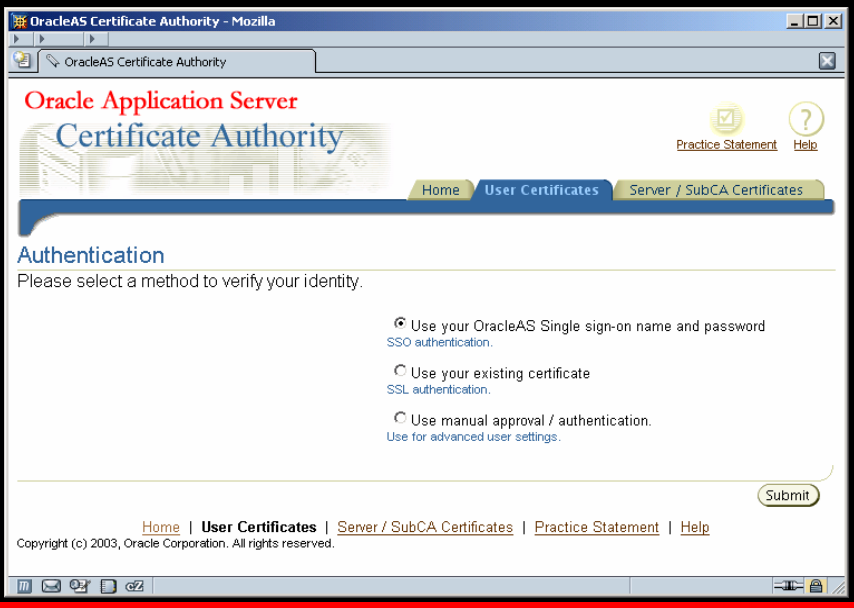


ORACLE

OracleAS 10g Oracle Certificate Authority



Oracle CA User Interface



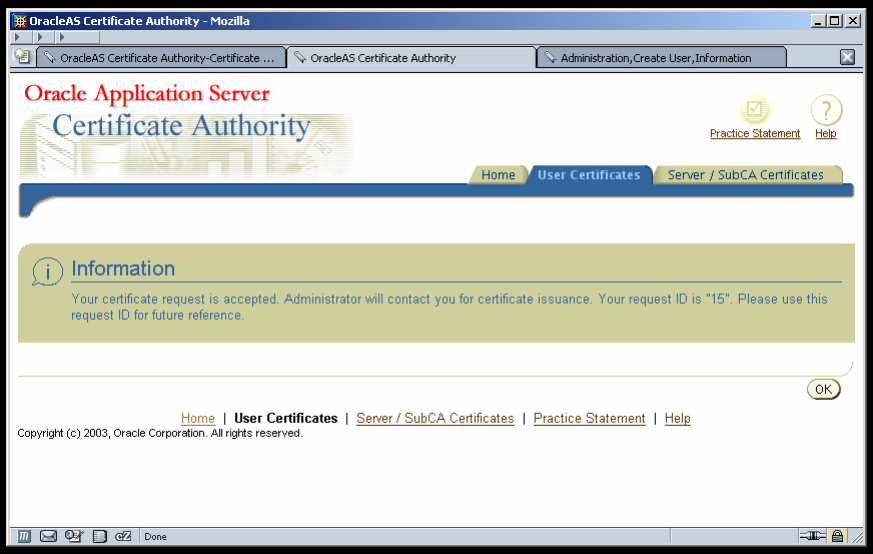
Anwender Zertifikate (manuell) 1

ORACLE

Benutzer Zertifikat (manuell) 2

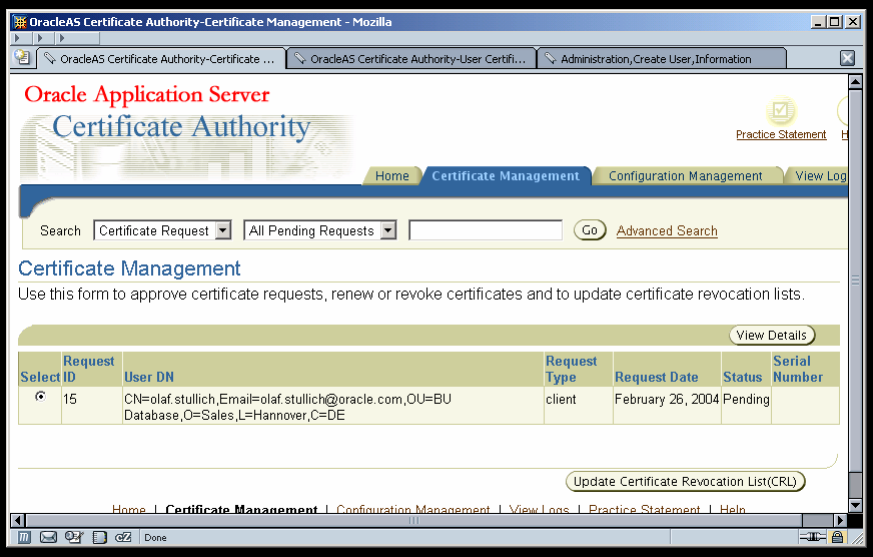
ORACLE

Benutzer Zertifikat (manuell) 3



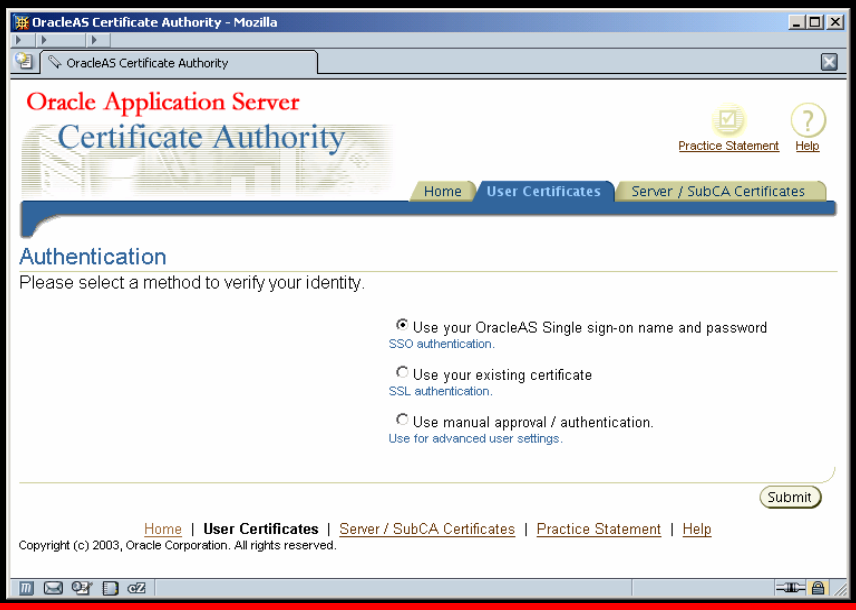
ORACLE

User Zertifikat (Admin Sicht)



ORACLE

Oracle CA User Interface

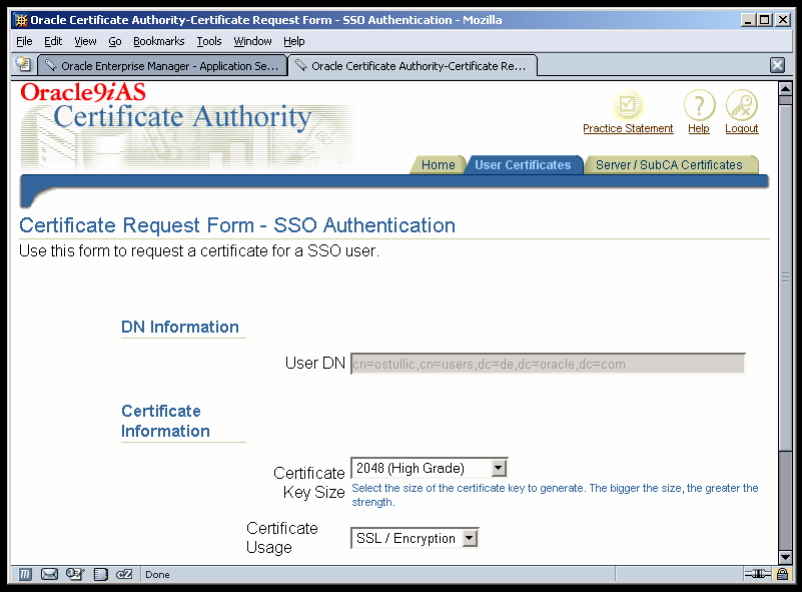


ORACLE

Benutzeranmeldung SSO

ORACLE

Request User Certificate



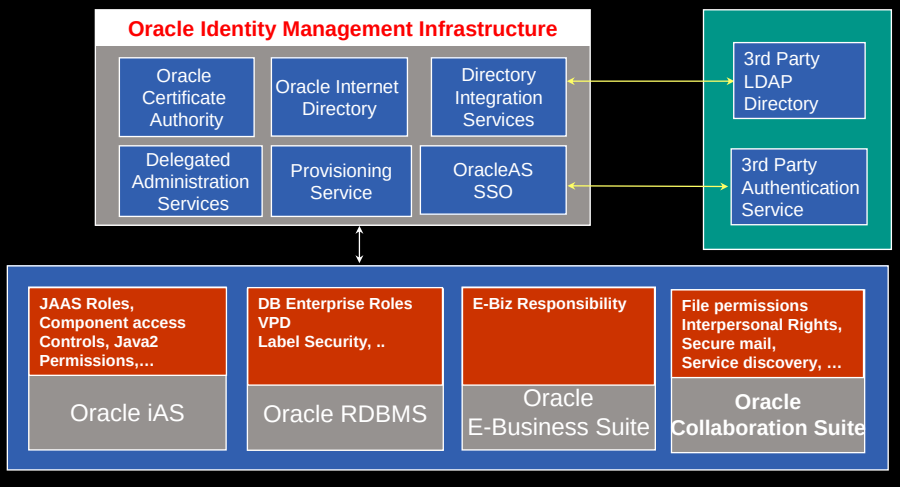
ORACLE

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

Oracle Identity Management



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

ORACLE


QUESTIONS
ANSWERS
ORACLE