

ORACLE®

Efektivní zabezpečení heterogenních systémů a přístupu k nim

Oracle Identity and Access Management

A decorative graphic consisting of a grid of white lines on a red-to-black gradient background, forming a perspective view of a grid.

David Matějů
Oracle Czech, s.r.o.

DATAKON
23. října 2005

ORACLE

ORACLE FUSION MIDDLEWARE

Cíle při zavádění IAM

- Centralizace všech uživatelských profilů do adresářové služby – LDAP
- Jednotná webová správa uživatelů a jejich přístupových práv
 - decentralizovaná (HR, manažeři / vedoucí, administrátoři)
 - procesní (podporující / vynucující definované bezpečnostní politiky)
- Okamžitá propagace změn do všech systémů
- Jednorázové uživatelské přihlášení – Single Sign-On
- Bezpečnostní audit a reporting



Internet

Extranet

Intranet

Portal



SSL, VPN



HR system



Oracle COREid Federation

Identity Federation to other systems

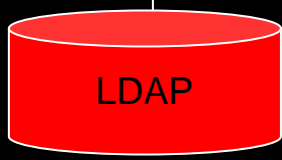
Identity and Access Management
Identity Workflow

Oracle COREid Access and Identity

Oracle COREid Provisioning

Provisioning

Oracle Internet Directory nebo jiný LDAP server



Oracle COREid Access and Identity

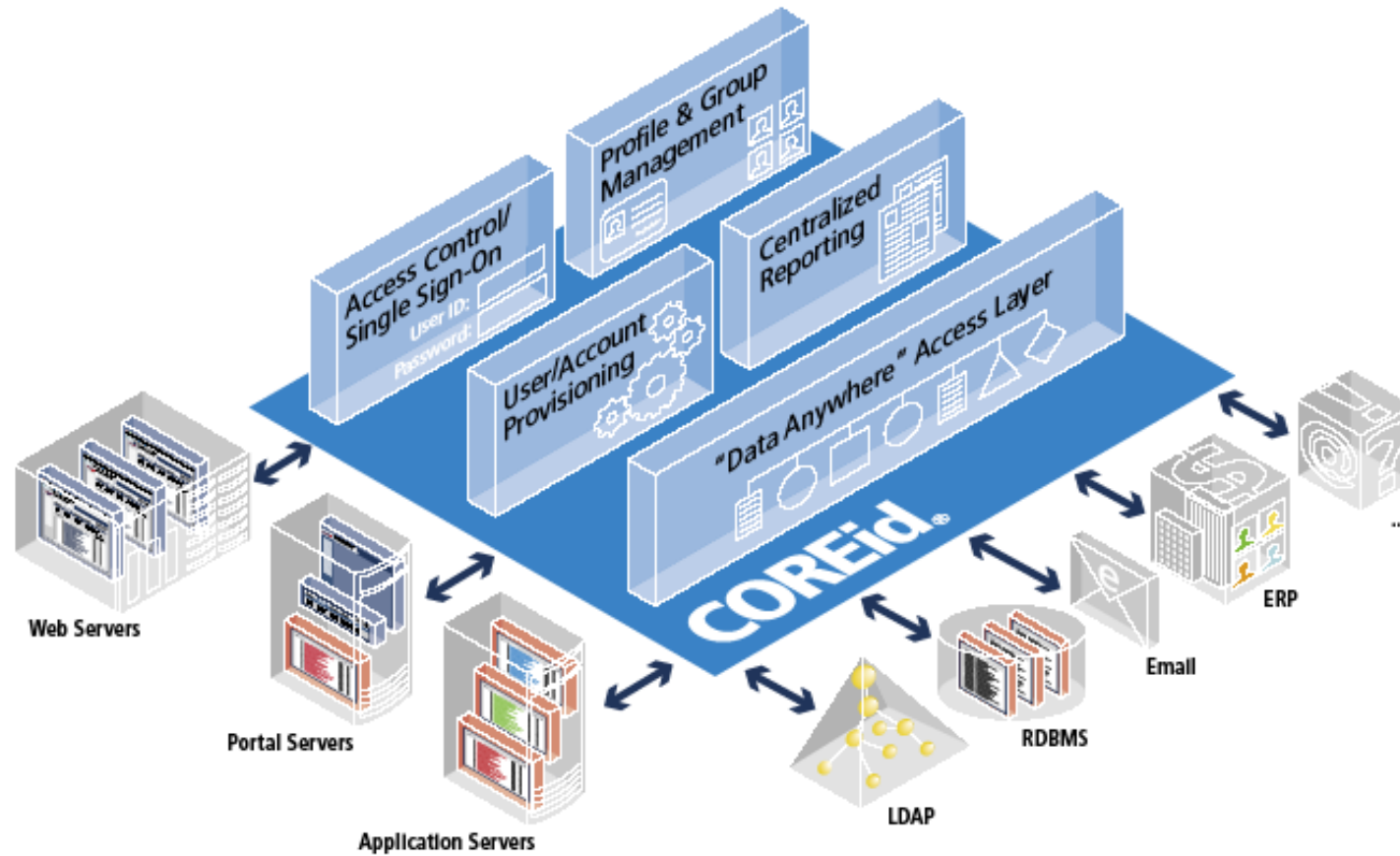
Audit

Oracle COREid Access and Identity

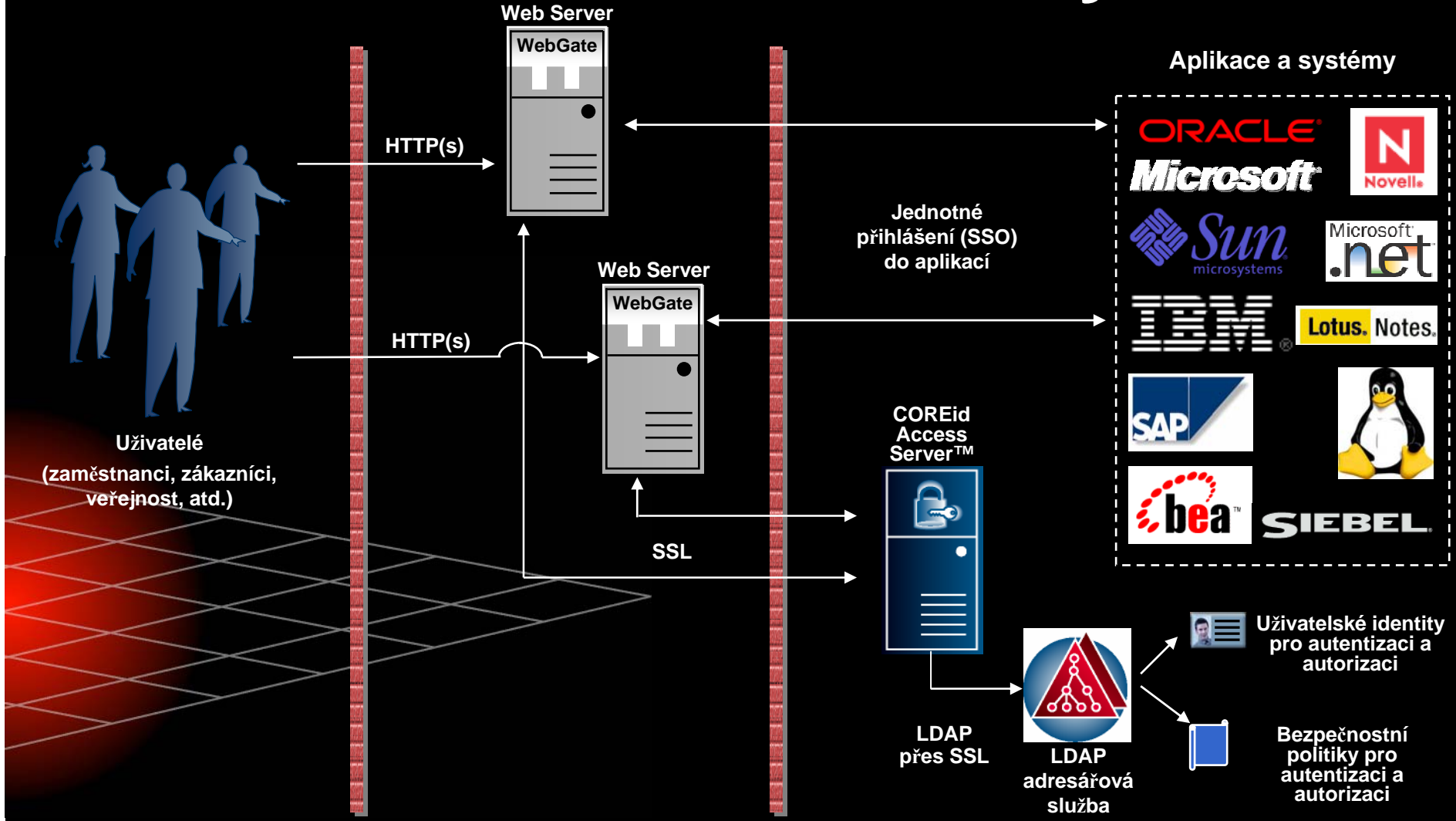
Reporting

- Web Servers & Applications
- Middleware Servers
- ERP, CRM
- Client / Server Applications
- LDAPs Databases
- Email Systems
- Operating Systems





COREid Access & Identity

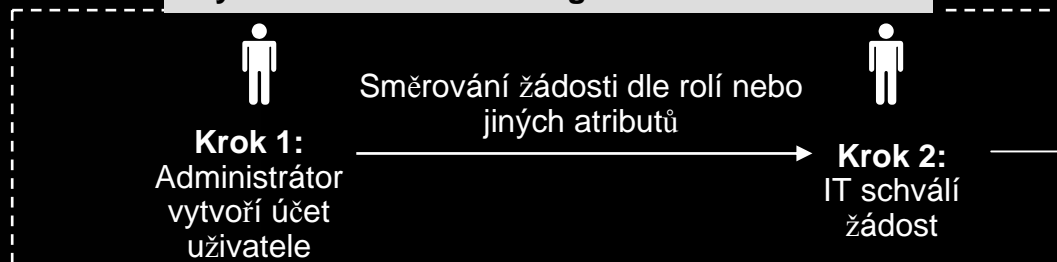


COREid Identity Workflow

Vytvoření uživatele: samoregistrace



Vytvoření uživatele: delegovaná administrace



Změna atributu



Flexibilní vícezkrokové workflow:
Pro každý proces lze definovat specifické workflow.





COREid Audit & Reporting

- Více než 200 předpřipravených reportů
 - Statistiky přes všechny servery
 - Dle uživatele
 - Dle zdroje IS
 - Detailní pohledy
- Možnost definice vlastních reportů

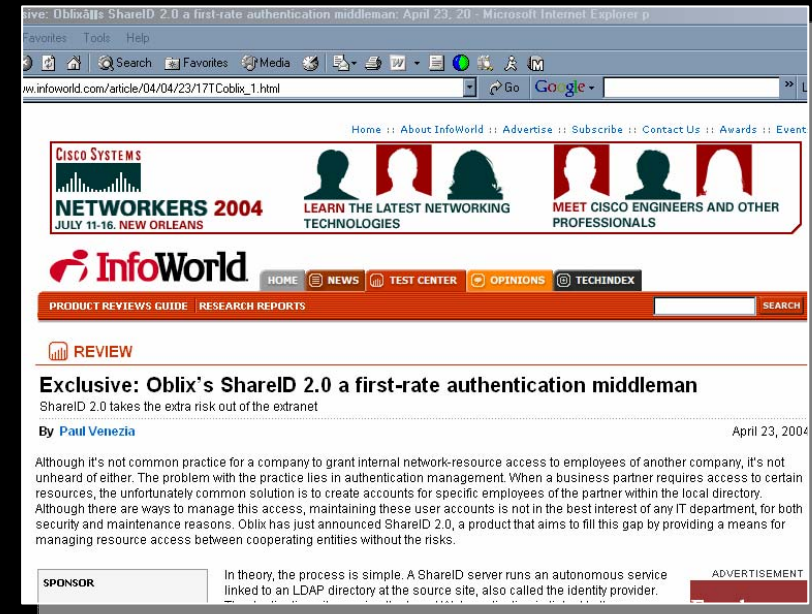
Authentication Statistics				
Date of creation 4/8/2004			Page 1 of 3	
Access Server Identifier : AAA1				
Authentication Success				
Time of Access	Resource Accessed	WebGate	Id	User
2/15/2004 9:15:28AM	/identity/oblix	wg1		cn=Rohit Valiveti, ou=Sales, ou=Dealer1k1, ou=Latin America, ou=Ford, o=Company, c=US
2/15/2004 9:15:29AM	/identity/oblix/apps/Userservcenter/bin/Userservcenter.cgi	wg1		cn=John Valiveti, ou=Sales, ou=Dealer1k1, ou=Latin America, ou=Ford, o=Company, c=US
2/15/2004 9:16:28AM	/identity/oblix	wg1		cn=Arun Valiveti, ou=Sales, ou=Dealer1k1, ou=Latin America, ou=Ford, o=Company, c=US
2/15/2004 9:16:29AM	/identity/oblix/apps/Userservcenter/bin/Userservcenter.cgi	wg1		cn=Smarto Valiveti, ou=Sales, ou=Dealer1k1, ou=Latin America, ou=Ford, o=Company, c=US
2/15/2004 9:16:55AM	/access/oblix	wg1		cn=Arun Valiveti, ou=Sales, ou=Dealer1k1, ou=Latin America, ou=Ford, o=Company, c=US
2/15/2004 9:16:56AM	/access/oblix/apps/admin/bin/front_page_admin.cgi	wg1		cn=Smarto Valiveti, ou=Sales, ou=Dealer1k1, ou=Latin America, ou=Ford, o=Company, c=US
2/15/2004 10:15:28AM	/identity/oblix/apps/groupservcenter/bin/groupservcenter.cgi	wg1		cn=Paddy Sharma, ou=Sales, ou=Dealer1k1, ou=Latin America, ou=Ford, o=Company, c=US
2/15/2004 10:16:28AM	/identity/oblix/apps/groupservcenter/bin/groupservcenter.cgi	wg1		cn=Sharad Chavali, ou=Sales, ou=Dealer1k1, ou=Latin America, ou=Ford, o=Company, c=US
2/15/2004 10:16:55AM	/access/oblix/apps/admin/bin/front_page_admin.cgi	wg1		cn=Sharad Chavali, ou=Sales, ou=Dealer1k1, ou=Latin America, ou=Ford, o=Company, c=US
2/15/2004 7:15:18PM	/identity/oblix/apps/objservcenter/bin/objservcenter.cgi	wg1		cn=Rambo, ou=Sales, ou=Dealer1k1, ou=Latin America, ou=Ford, o=Company, c=US
2/15/2004 7:16:15PM	/access/oblix/apps/admin/bin/front_page_admin.cgi	wg1		cn=Rekha Shinde, ou=Sales, ou=Dealer1k1, ou=Latin America, ou=Ford, o=Company, c=US
2/15/2004 7:16:18PM	/identity/oblix/apps/objservcenter/bin/objservcenter.cgi	wg1		cn=Rekha Shinde, ou=Sales, ou=Dealer1k1, ou=Latin America, ou=Ford, o=Company, c=US
Total		12		
Authentication Failure				
Time of Access	Resource Accessed	WebGate	Id	User
2/15/2004 9:14:55AM	/access/oblix	wg1		-----
2/15/2004 9:14:56AM	/access/oblix/apps/admin/bin/front_page_admin.cgi	wg1		-----
2/15/2004 10:14:55AM	/access/oblix/apps/admin/bin/front_page_admin.cgi	wg1		-----
2/15/2004 7:14:15PM	/access/oblix/apps/admin/bin/front_page_admin.cgi	wg1		-----
Total		4		

ORACLE

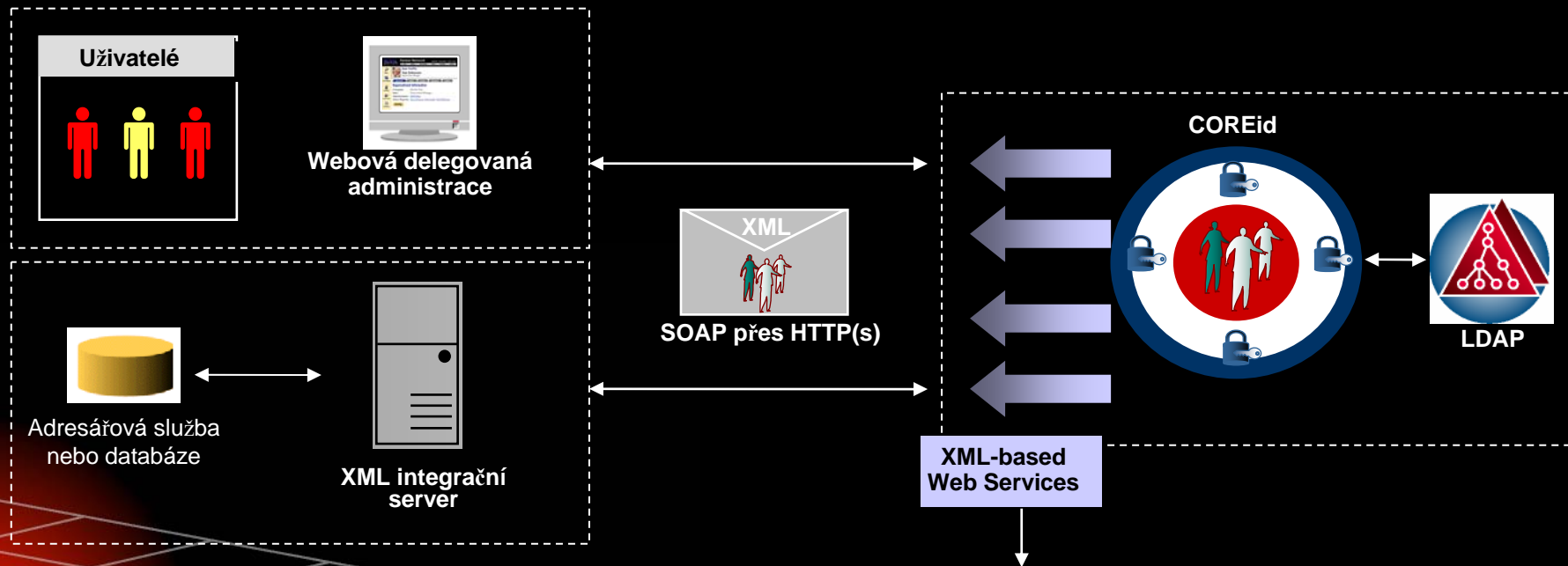
ORACLE FUSION MIDDLEWARE

COREid Federation

- Bezpečný mechanismus pro sdílení identit v rámci více organizací
- Podpora standardů SAML, WS-Federation, Liberty Alliance*
- V roce 2004 zvolen jako standard pro státní správu v US



Podpora webových služeb



COREid IdentityXML

- Správa uživatelů a jejich identit
- Správa skupin a jejich identit, přiřazování do skupin
- Správa organizační struktury
- Identity Management Workflow
- Standardní WSDL/UDDI rozhraní

Přínosy Oracle IAM

- ✓ Nejen technologie, ale i know-how
 - ✓ procesy, reporty
- ✓ Neomezená delegovaná administrace centrálního úložiště
- ✓ Ochrana investic – podpora současných systémů
 - ✓ platformy, OS, databáze, LDAP servery, aplikační servery, aplikace
- ✓ Plná podpora WS a XML pro snadnou integraci produktů třetích stran
- ✓ Podpora SmartCard, RSA SecurID, atd.

Bezpečnost? Oracle!

Bezpečnostní certifikáty – Databázové servery

Bezpečnostní kritérium	Oracle	Microsoft	IBM DB2
TCSEC, level B1	1	0	0
TCSEC, level C2	1	1	0
ITSEC Levels E3/F-C2	3	0	0
ITSEC Levels E3/F-B1	3	0	0
Russian Criteria, levels III, IV	2	0	0
CC level EAL-4, ISO 15408	6	0	1
US FIPS-140, level 2	1	0	0
CELKEM	17	1	1

ORACLE

ORACLE FUSION MIDDLEWARE



Finanční služby

- » Northern Trust
- » Washington Mutual
- » Penn Mutual
- » Chicago Board of Trade
- » Bank Lombard
- » AXA Financial
- » Charles Schwab
- » CUNA Mutual Group
- » Farmer's Group
- » Maritime Life
- » Mass Mutual
- » Morgan Stanley Dean Witter
- » Old Mutual
- » Paine Webber
- » Thomas Weisel Partners
- » Wachovia
- » **Volkswagen Credit**

Výroba a obchod

- » Best Buy
- » Blockbuster
- » Burger King
- » Aventis
- » **General Motors**
- » **Daimler Chrysler**

Technologie

- » **Cisco Systems**
- » Conexant
- » Corio
- » **Dell Computer**
- » Fujitsu Networks
- » Hitachi Computers
- » i2 Technologies
- » Intuit
- » Opware (Loudcloud)
- » Symantec
- » Xircom

Transport a logistika

- » American Airlines
- » American President Lines
- » **British Airways**
- » Southwest Airlines
- » **Fed Ex**
- » CEMEX
- » Norsk Hydro
- » CP Ships

Farmacie

- » **Pfizer**
- » Kaiser Permanente
- » SSHA Canada

Vládní a státní instituce

- » **US Postal Service**
- » Federal Reserve Bank
- » Intelligence Community
- » Aerospace Corporation
- » SPAWAR – US Navy
- » Air Force Research Labs
- » UK Inland Revenue
- » **Government of Belgium**
- » State of Minnesota
- » State of New Jersey
- » State of North Carolina
- » State of New Mexico
- » CUNY
- » UCSB
- » Danish Immigration
- » **NASA**
- » Colorado Springs Utilities
- » Duke University
- » Stanford University

Telekomunikace

- » AT&T Wireless
- » MCI
- » **Nokia**
- » **Telefonica**
- » Tellabs
- » Allstream

ORACLE

ORACLE FUSION MIDDLEWARE

Informace a kontakt

- <http://otn.oracle.com>
- david.mateju@oracle.com



OTÁZKY
ODPOVĚDI

ORACLE

ORACLE®