

Identity Management

centralizovaná správa uživatelů

AMI Praha a.s. - Tomáš Faško, výkonný ředitel | 17. března 2010

Miroslav Rusko, account manager

Martin Lízner, specialista pro Identity Management

1. Úvod, představení
2. Problematika správy uživatelů
3. SUN Java Identity Management
4. Reference
5. Kontakt

AMI Praha a.s.

- systémový integrátor
- vývoj aplikací J2EE
- tvorba a správa internetových prezentací
- SW partner SUN Microsystems/ORACLE, Adobe, Asseco, Aplis

www.ami.cz

- „Životní cyklus uživatele“

Nový zaměstnanec přicházející do podniku

- Vložení informace o zaměstnanci do systému správy lidských zdrojů (HR)
- Poskytnutí účtů podnikovým systémům & aplikacím
- Přidělení a/nebo inicializace nedigitálních identifikátorů (mobilní telefony, karty pro vstup do budov atp.)

Změny & uživatelská podpora

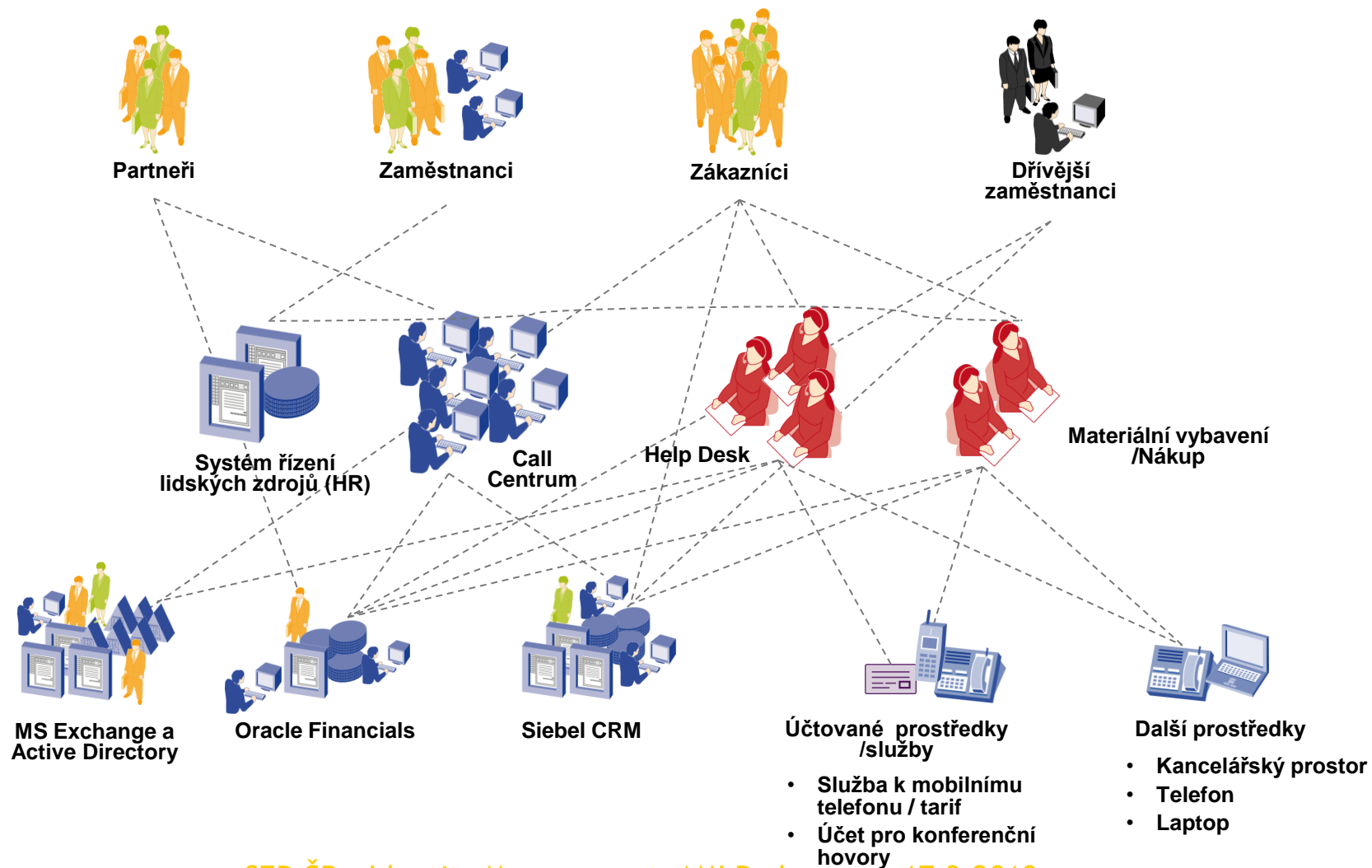
- Změny pracovního zařazení/role/statutu
- Změny a resety hesel
- Změny informací v osobním profilu
- Další požadavky na přístupová práva účtu nebo nedigitálních identifikátorů

Zaměstnanec opouštějící podnik

- Aktualizace statutu zaměstnance v HR systému
- Zablokování & odstranění účtu
- Vrácení a/nebo zrušení nedigitálních identifikátorů

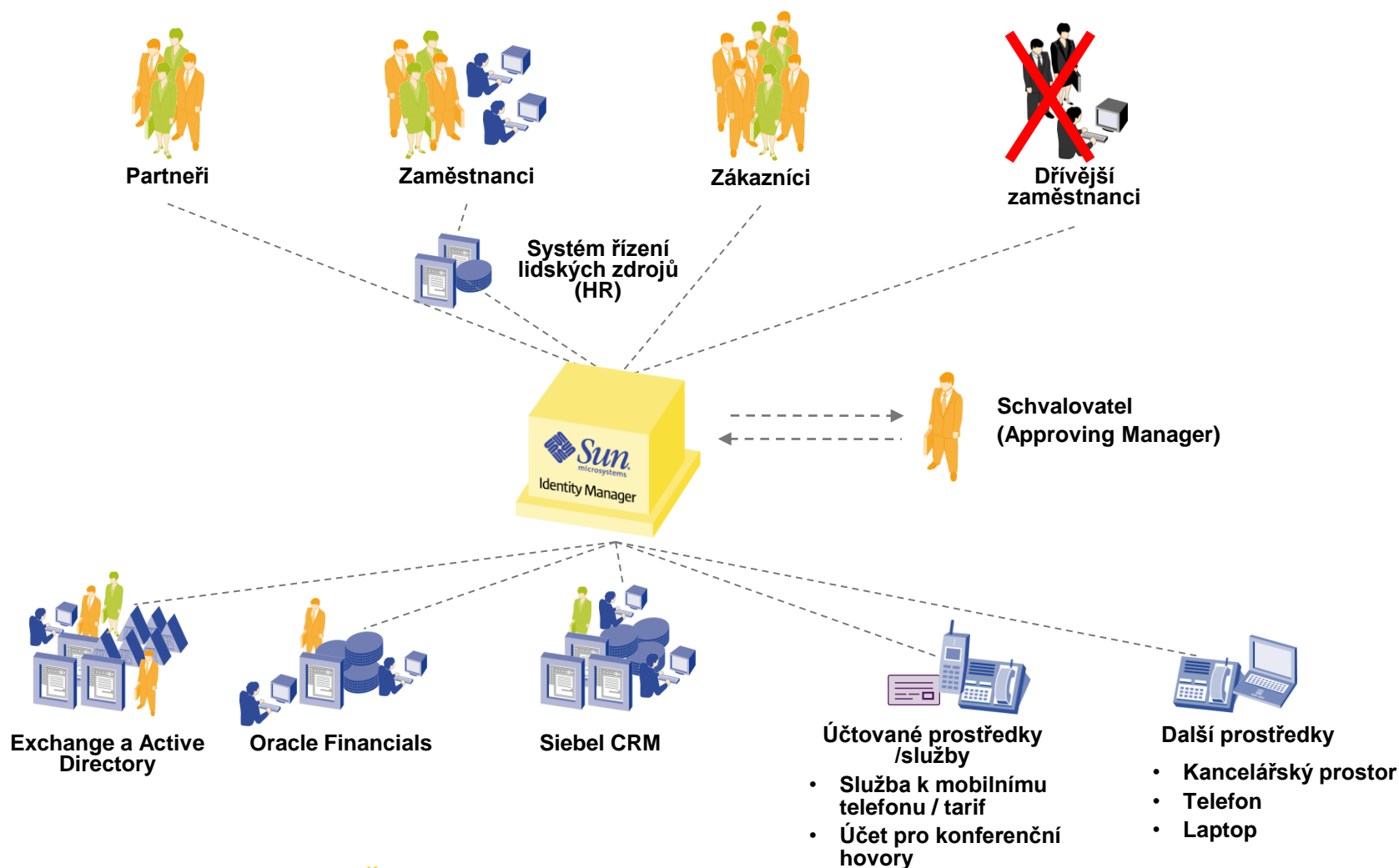


Problematika správy uživatelů



- Proces správy uživatelských účtů
 - pracný
 - dlouhotrvající
 - rizikový (lidský faktor)
 - omezené možnosti pro kontrolu přístupů

Problematika správy uživatelů



Přehled funkcionalit nástrojů IdM:



Automatizovaný provisioning

- vytváření, změny a rušení uživatelských účtů na koncových systémech na základě definovaných pravidel
- autoritativním systémem HR nebo jiné úložiště (DB, LDAP, ale i samotné IdM)
- přístupová oprávnění na základě rolí, předpokladem je definice business rolí v organizaci

Samooobslužné nástroje

- změna hesla, vynucování politiky hesel
- žádost o role nebo oprávnění
- změna osobních údajů

Audit

- na základě údajů z IdM okamžitý reporting jako podklad pro bezpečnostní audit (kdo má kam jaká oprávnění)

Důvody pro nasazení automatizovaných nástrojů IdM:



Snižování nákladů

- Nízká provozní efektivita oddělení lidských zdrojů, IT, materiálního vybavení a dodavatelů způsobená: manuálními procesy, papírovými dotazníky, emaily, telefonními voláními
- Stoupají náklady na provádění resetu hesel prostřednictvím helpdesku

Zvýšené vnímání bezpečnosti

zapomenuté spící účty představují značná rizika

- Umožňují kybernetické útoky
- Končí neúspěšným auditem

Závazné směrnice:

Směrnice Evropského parlamentu a Rady, Basel II, Sarbanes-Oxley, HIPAA, GLB, 21 CFR Part 11, Canadian Privacy Act — vyžadují bezpečnou správu přístupu

- J2EE aplikace
- platformově nezávislá aplikace (OS, DB)
- bezagentová technologie
 - není nutné nic instalovat na ovládané systémy
- UI tenký klient MSIE, Mozilla
- Workflow
- adaptéry na více než 50 systémů (OS, DB, aplikace)
- podpora standardů

Doporučený postup nasazování IdM



1. Analýza procesů a prostředí

- požadavky na správu uživatelů z provozního a bezpečnostního hlediska
- návrh na úpravu procesů spojených se správou uživatelských oprávnění
- výběr reprezentativních systémů

2. Implementace vybraných systémů

- zavedení IdM
- změna procesů
- definice business rolí

3. Rollout na další systémy

- postupné připojování dalších systémů k IdM

- CCS Česká společnost pro platební karty
- UniCredit Leasing (CAC LEASING)
- Lesy ČR
- ČEZ
- Česká Pošta



AMI Praha a.s. - www.ami.cz obchod@ami.cz

Pláničkova 11, Praha 6, 162 00, tel. + 420 274 783 239

Tomáš Faško - tomas.fasko@ami.cz

výkonný ředitel

Miroslav Rusko - miroslav.rusko@ami.cz

account manager

Otázky a odpovědi