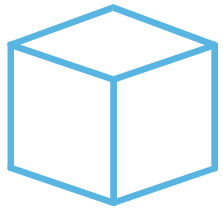
Riešenia a technológie pre jednotnú správu používateľov

Radovan Semančík



BGS
Business Global Systems

Agenda

- Úvod: Identity Crisis
- Technológie správy používateľov
- Postup nasadenia
- Záver

Súčasný stav IT Security

- Nekonzistentné bezpečnostné politiky
- Nekonzistentné databázy používateľov
- Perimeter security je neefektívna
- Rýchle vírusové infekcie
- Útoky z vnútra organizácie
- Patching doesn't work
- **Identity Crisis**

Identity Crisis

- Nikto nevie, kto má mať kam prístup
- Nikto nevie, kde všade má zamestnanec prístup
- Prístupy na firewall/VPDN iné ako do IS
- Mobility vs Security
- Vysoké náklady: help desk, prestoje, zmeny

It's clear identity has become a strategic business issue, not just a technology issue.

-- Jamie Lewis, president of consultancy Burton Group

Mýtus centralizácie

- Jedna databáza/directory/čokoľvek
  - Rýchlo nekonzistentná
  - Nákladné na údržbu
  - Bezpečnostné riziko
  - Nie vždy technologicky možné (SQL join, offline, ...)
- Nutná synchronizácia
- Nekonzistencia
  - Rôzne UID
  - Rôzne typy prístupových práv
  - Neexistuje štruktúra rolí

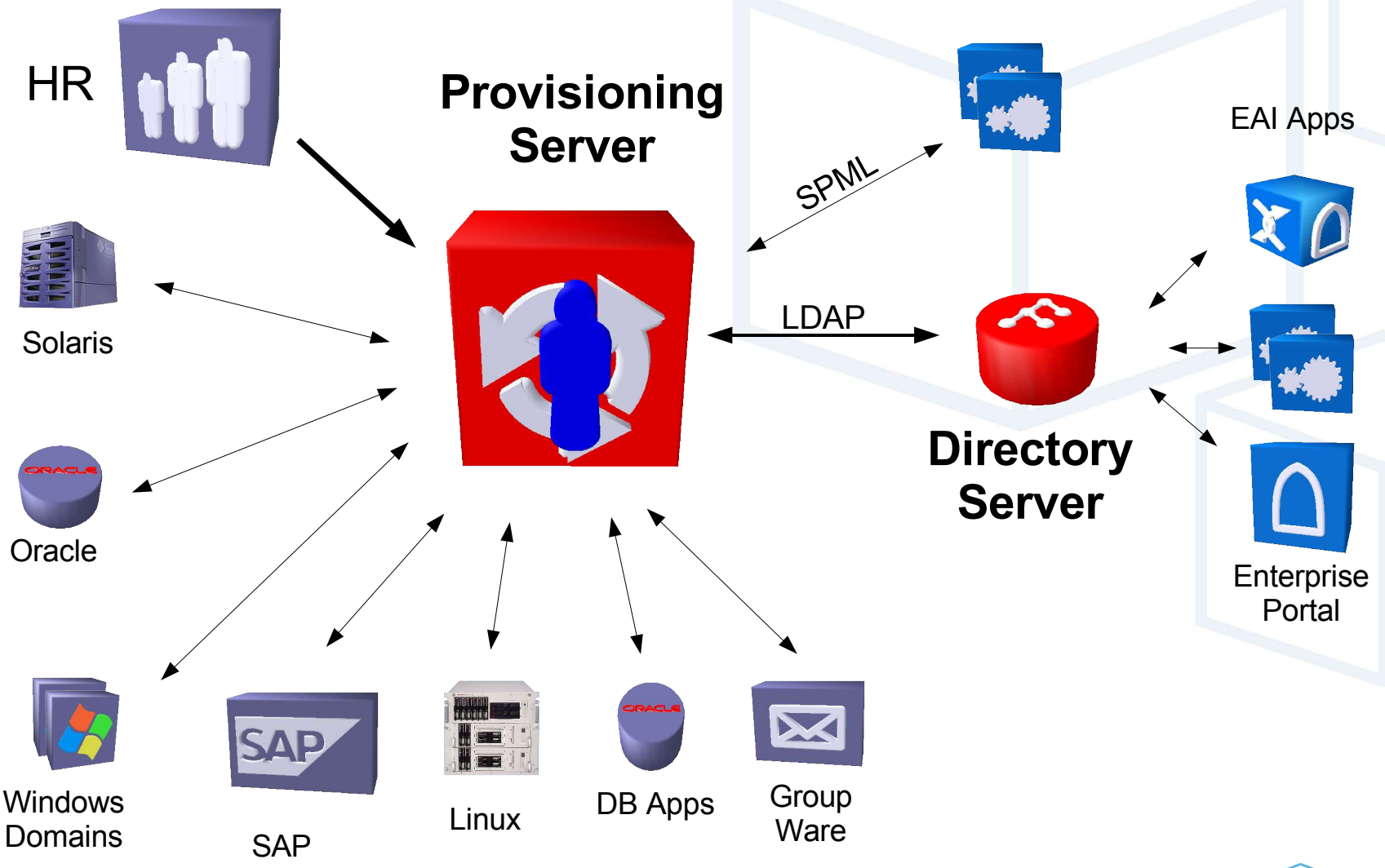
Agenda

- Úvod: Identity Crisis
- Technológie správy používateľov
- Postup nasadenia
- Záver

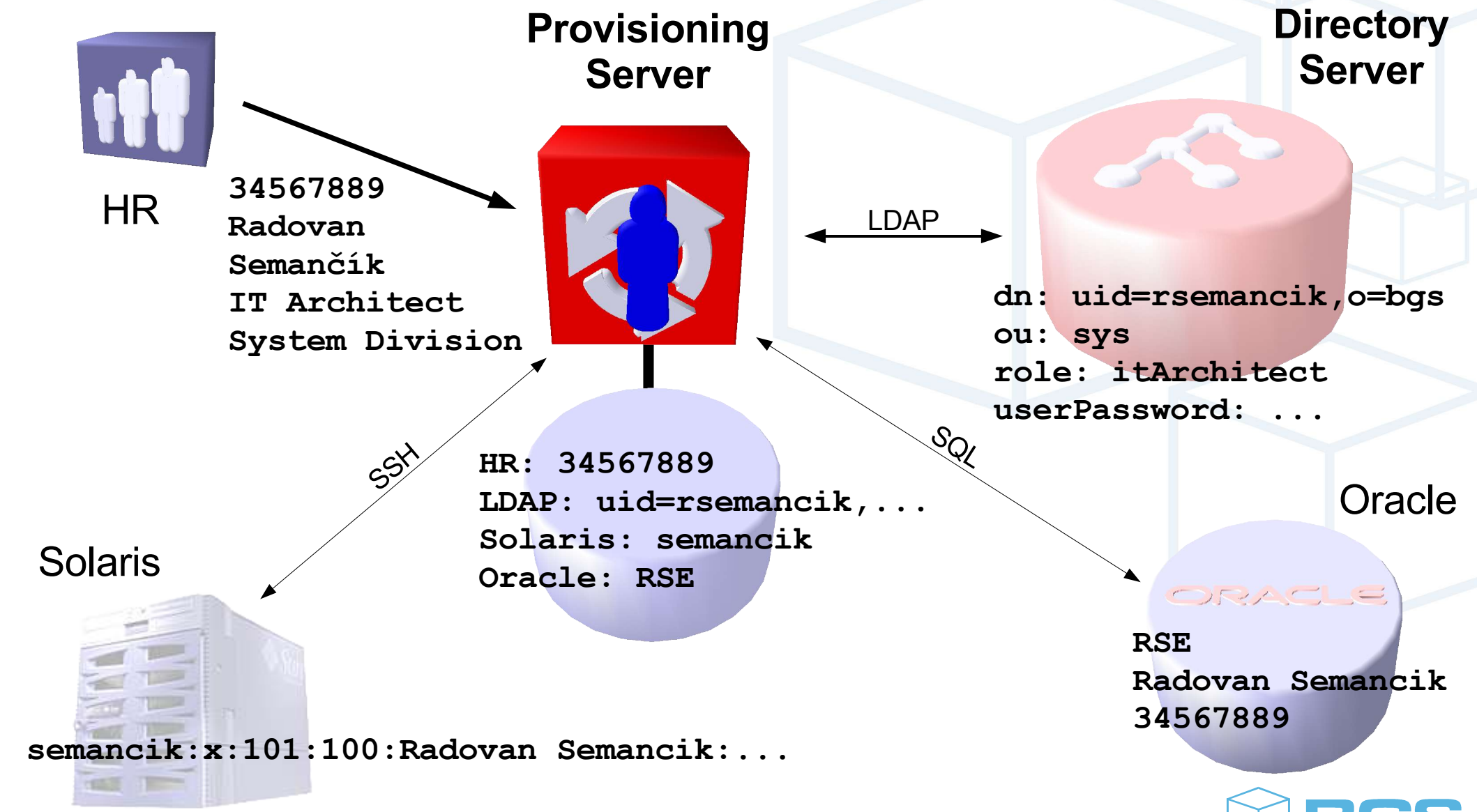
Technológie správy používateľov

- **Directory Server (LDAP)**
  - Nutná podmienka, nie však postačujúca
  - Len databáza, žiadna inteligencia
- **Provisioning system**
  - Synchronizácia údajov, workflow
  - Organizačná štruktúra role
- Metadirectory
  - Jednoduché pravidlá, obmedzenia (rovnaké uid)
- User Management, Doménové systémy, ...
  - Jednoduché, jednoúčelové, prvý krok

User Provisioning

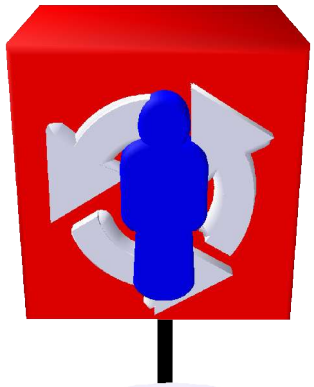


Spôsob práce Provisioning Servera



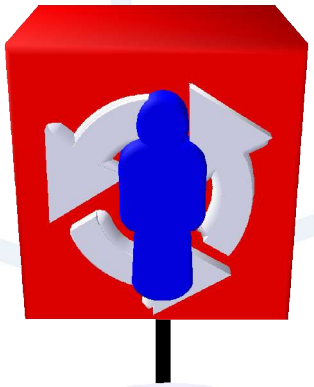
Databáza vs Metadata

Databáza



```
34567889
Radovan Semančík
IT Architect
System Division
uid: 101
```

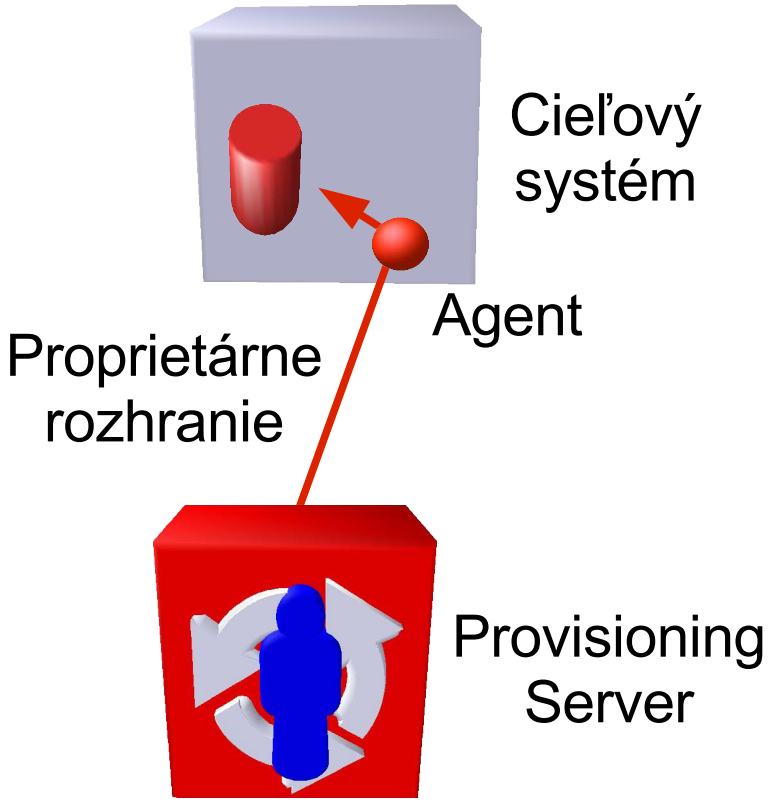
Metadata



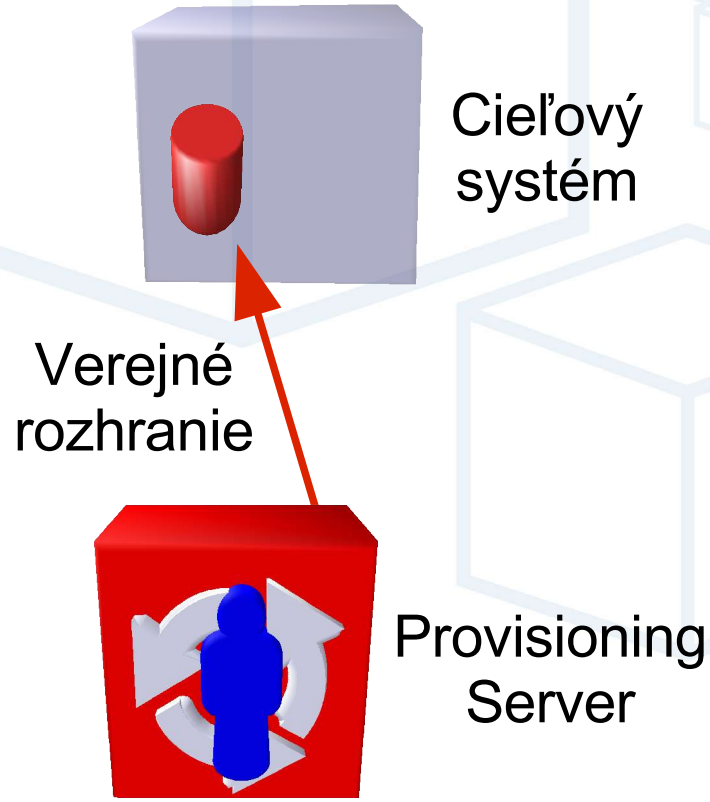
```
HR: 34567889
LDAP: uid=rsemancik,...
Solaris: semancik
Oracle: RSE
```

Agenti vs Rozhrania

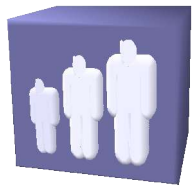
Agentový prístup



Bezagentový prístup



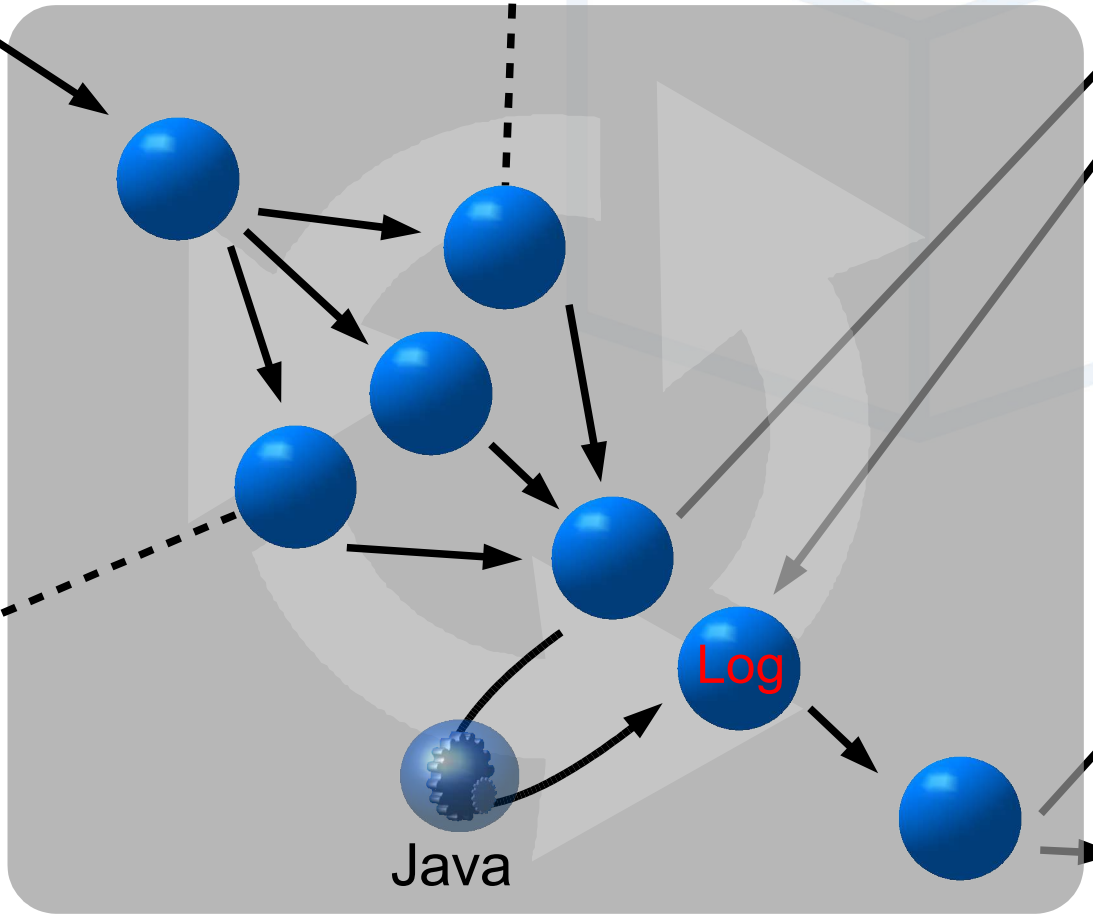
Workflow

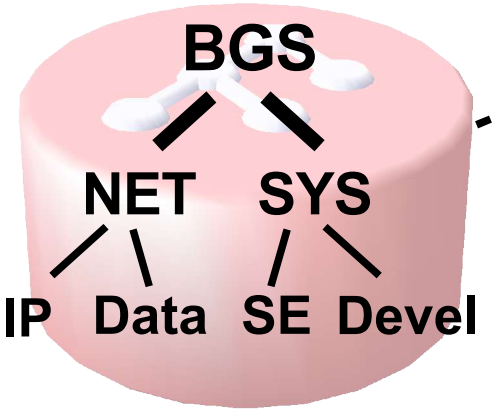


HR

34567889
Radovan
Semančík
IT Architect
System Division

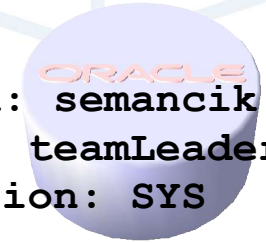
WfMC
TC-1023





Directory
Server

semancik:x:101:..
group: admin



login: semancik
role: teamLeader
division: SYS

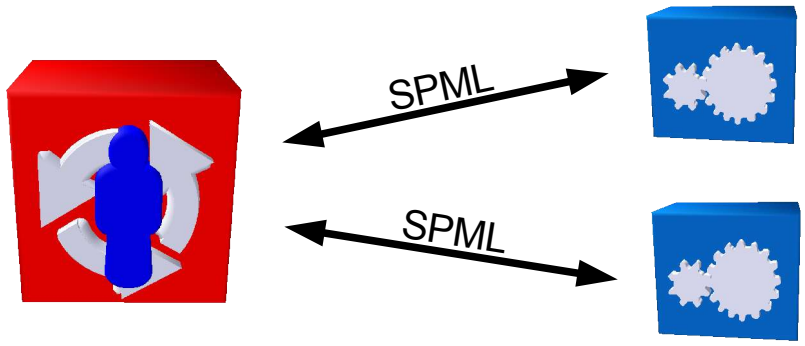
BGS
Business Global Systems

Dôležité špecifikácie

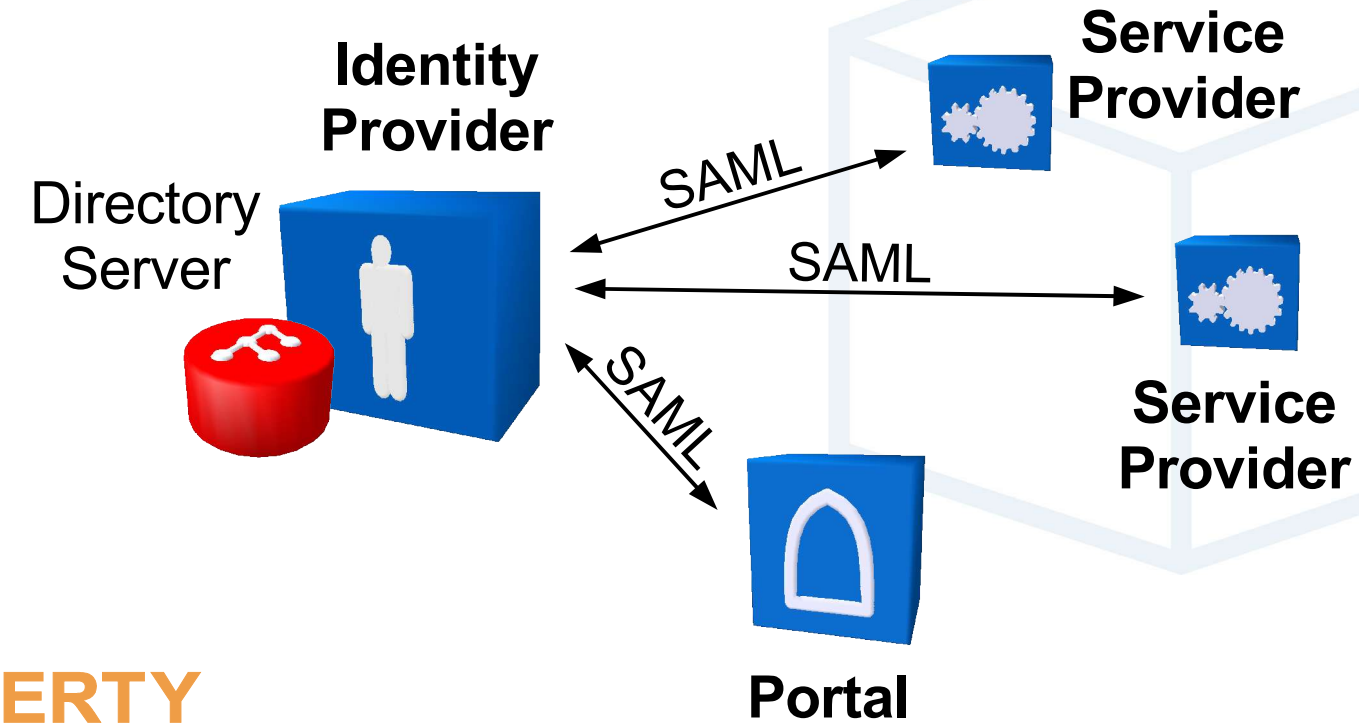
- Lightweight Directory Access Protocol (LDAP)
- Directory Services Markup Language (DSML)
- Service Provisioning Markup Language (SPML)
- Project Liberty Specification, Phase I
- Project Liberty Specification, Phase II
- WS-Security
- WS-Federation

Service Provisioning Markup Language

- Jazyk pre Provisioning systémy založený na XML
- Štandardizácia: OASIS Provisioning Services Technical Committee
- Založené na DSMLv2, spolupracuje so SAML a WS-Security
- Štandardné rozhranie – ľahká integrácia



Liberty Alliance Project



LIBERTY ALLIANCE

Agenda

- Úvod: Identity Crisis
- Technológie správy používateľov
- Postup nasadenia
- Záver

User Management Projects

- **Central User Management Project**
  - Centrálna správa zamestnaneckých prístupov
  - Výrazné finančné šetrenie
  - Provisioning Server (Sun Java System Identity Manager)

- **Customer Identity Management Project**
  - Správa zákazníckych prístupov
  - Veľké množstvo záznamov, málo systémov
  - Metadirectory, Directory-based replikátory

Digital Identity Projects

- **Single Sign-On Project**
  - Intra-enterprise systematic SSO
  - Základ komponentu pre SOA
  - SSO server (Sun Java System Access Manager)

- **Digital Identity (Federation) Project**
  - Externé (internet) SSO
  - Externé zdieľanie atribútov
  - Identity Provider

Agenda

- Úvod: Identity Crisis
- Technológie správy používateľov
- Postup nasadenia
- Záver

Záver

- Jednotná správa používateľov je prvý nutný krok
- Single Sign-On a Digital Identity až potom
- Orientácia na štandardy
- Dobrá architektúra

> It is possible to deploy identity in incremental steps, but you won't succeed if you haven't built an overall plan before you start.
>
> -- Phil Becker, Digital ID World

Otázky

Ďakujem za pozornosť

Ing. Radovan Semančík

Business Global Systems, a.s.
Pluhová 2
83248 Bratislava

semancik@bgs.sk