Principles of Building e-Security for Public e-Services

Rado Majerský
Director of Infrastructure Solutions Group
PosAm Ltd.

14.XI.2006, Bratislava
Congress itapa 2006

PosAm

Agenda

- Global (ICT) Trends
- IAM Segment – Overview
- Governmental Digital Identity – Current Status
- Digital Identity – Common Problems
- Implementing Digital Identity - Recommendations
- VALUE for Our (Government) Customers
- References

PosAm

Global (ICT) Trends

- **Challenge to Reduce Costs (TCO)**
- **Pressure on Fast Return On Investments (ROI)**
- **Globalization and Consolidation (Acquisitions, Mergers..)**
- **Slovakia and EU Relationship (EC Directives, SK laws)**
- **Emphasis on Security Influenced by Global Events and Legislation (11/IX/2001, Sarbanes-Oxley Act, Basel II)**
- **Development of NEW Segment on ICT Market – IAM**

IAM Segment - Overview

- **(I) Reducing Costs of ICT Infrastructure Management,**
- **(II) Increasing Security,**
- **(III) Improving Quality of Services.**

PosAm

Governmental Digital Identity – Current Status

- **Digital Signature**
  - codified in Europe by the Directive 1999/93/EC [2], which was applied to EU local legislations,
  - Directive specifies only the mechanism for digital signature creation and validity.
- **People Identification and Personal Data Management**
  - framework partially set by the Directive 95/46/EC [3], that specifies the rules concerning the personal data transfer and processing.
- **Inconsistency of Governmental Systems [4]**

PosAm

Digital Identity – Common Problems

- **Global Identifiers**
  - Many systems use GIs to identify users, such as Social Security Numbers, URLs or e-mail addresses.
  - GIs allow different sites to correlate information about users, which usually allows sites to gain more information that was specifically allowed by the user.
- **Insecure Workstations**
  - The typical user's workstation used for Internet access is not a secure environment.
  - Viruses and other malware can easily infect the workstation and gain control over all user's activities (observed passwords, mounted authentication mechanisms,

PosAm

Digital Identity – Common Problems (part II)

- **Honeypot effect**
  - Centralizing personal information in one place may be very convenient from the data management point of view, but such repository may create a very attractive target for attackers.
  - The effect is the same if the information is stored on the governmental servers, hosted by the Internet identity providers or kept on the user's workstation.

PosAm

Implementing Digital Identity – Recommendations [1]

- ***(I) Assessment of Identity Information Repositories,***
- ***(II) Deployment of Provisioning System,***
- ***(III) Creation of Central User Database,***
- ***(IV) Implementation of Single Sign-On,***
- ***(V) Deployment of Attribute Services,***
- ***(VI) Federation.***

PosAm

Implementing Digital Identity

- ***(I) Assessment of Identity Information Repositories***

  - ***Make a quick analysis of your information assets and resources: user databases, organizational structure, user management procedures, legislative regulations, etc.***

  - ***The results will help in defining the requirements and scope of following steps.***

PosAm

Implementing Digital Identity

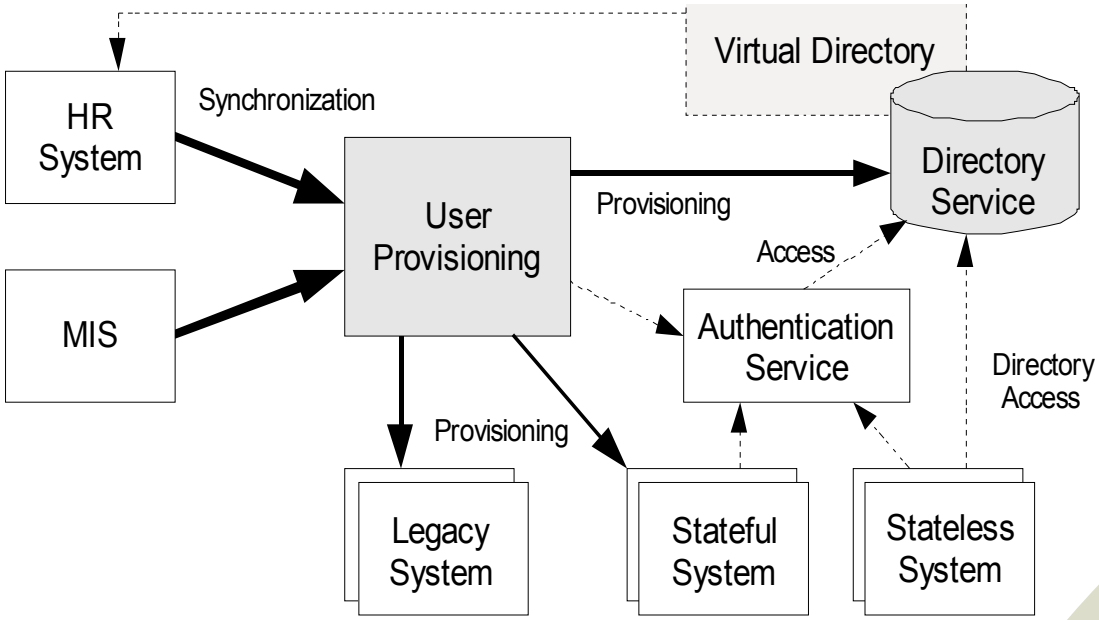
- ***(II) Deployment of Provisioning System***

  - ***Automate and refine your user management procedures by implementing user provisioning system.***
  - ***Cleverly customized workflow engine that follows the dynamic organizational structure is usually the key here.***
  - ***Deployed provisioning system should provide tools for user database cleanup, the design and deployment of role-based access control mechanisms and end system monitoring.***

PosAm

Implementing Digital Identity

- ***(III) Creation of Central User Database***
  - ***Use the deployed provisioning system to create and maintain a central user database, usually as a replicated directory server. This database may act as an authoritative source for the systems in following steps.***



PosAm

Implementing Digital Identity

- ***(III) Creation of Central User Database***

  - ***Alternatively, use virtual directory or metadirectory techniques to create the central user database. The central user database is not central in the way that all systems must use it.***

  - ***The database is supposed to hold authoritative data that some important (usually infrastructure) services will use.***

PosAm

Implementing Digital Identity

- ***(IV) Implementation of Single Sign-On***
  - ***Using the central database implement Single Sign-On as the authentication service.***
  - ***The implementation of SSO may be quite straightforward for web applications and very complex for legacy applications.***

PosAm

Implementing Digital Identity

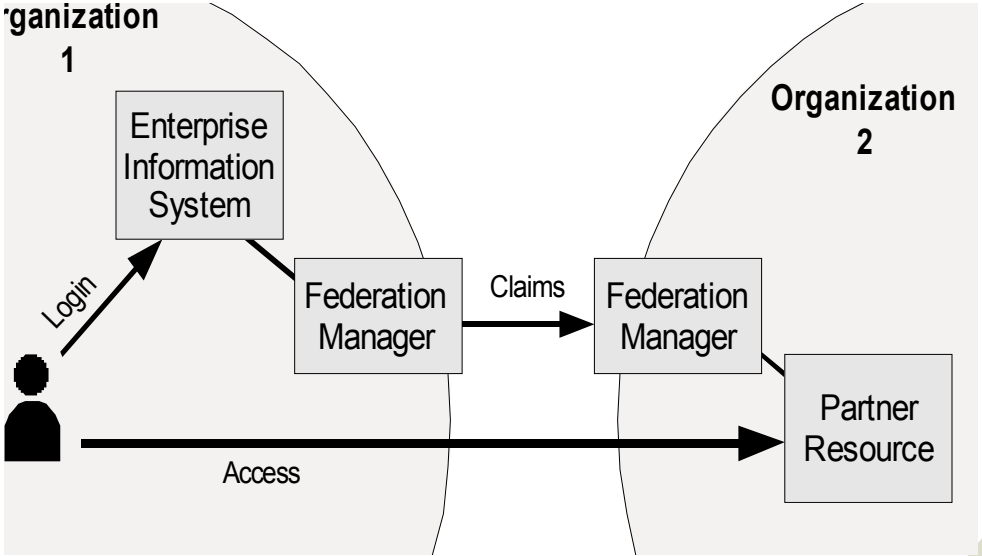
- ***(V) Deployment of Attribute Services***

  - ***Using central user database and authentication service. The simplest attribute service may be implemented by sharing parts of directory server with other applications.***
  - ***But as your Service Oriented Architecture evolve, more complex attribute services will be needed, most probably in the form of infrastructure web services.***
  - ***This allow the deployment of relatively lightweight services, that do not need to maintain their own user databases.***

PosAm

Implementing Digital Identity

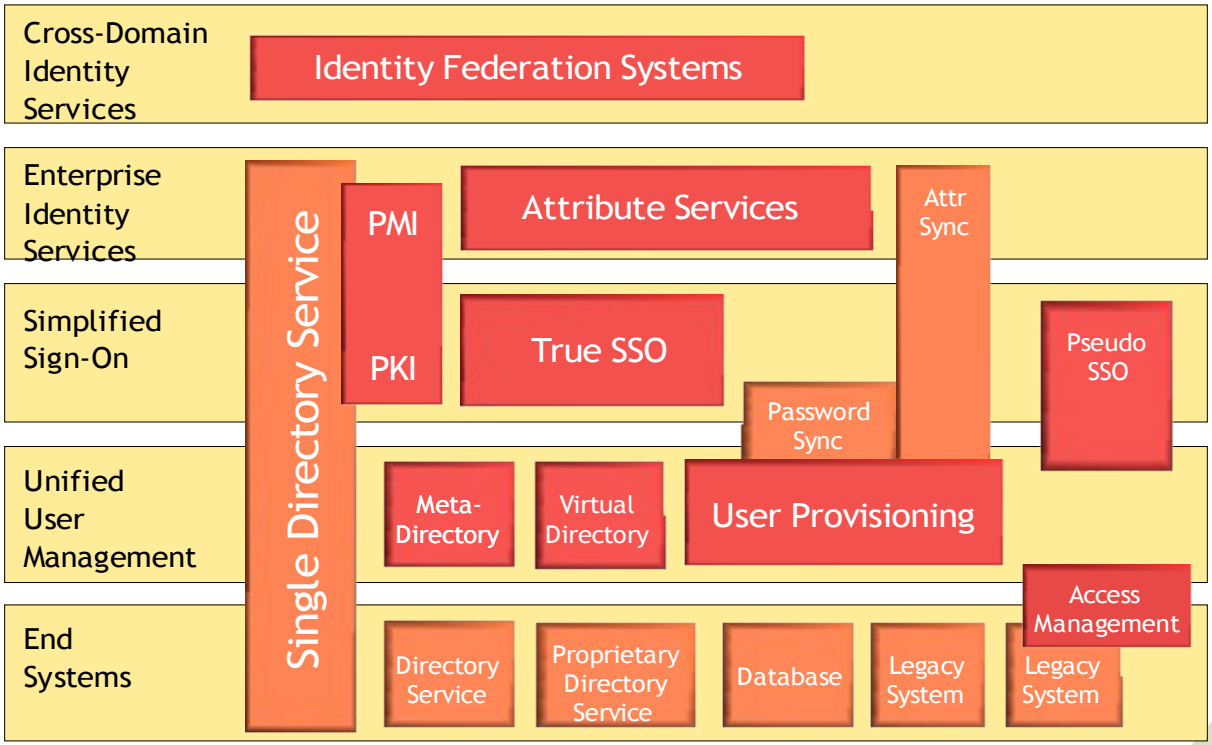
- ***(VI) Federation***
  - ***Connect your digital identity services with similar services in other organizations by joining a federation relationship.***
  - ***Use of federation allows better degree of cross-organizational cooperation.***



PosAm

Digital Identity – Conclusion

- **Existing IAM Technologies – No Complete Solution**
  - **The different identity management technologies can be assigned to identity management architectural layers, as illustrated on the figure below :**



PosAm

PosAm VALUES for (Gov't) Customers

- **Domain knowledge of Public Sector,**
- **Trained and Certified IAM Professionals,**
- **Real World Implementation Experience,**
- **Individual Attitude and Long-Term Relationship,**
- **Trust is Commitment,**
- **VALUE – Useful Ideas,**
- **VALUE – Useful Technologies..**

PosAm

THANKS

for your attention

and

wishing you good times

in the congress

itapa 2006

PosAm

majersky@posam.sk

REFERENCES

[0] **Majerský, R.:** ***Integrujeme najlepšie riešenia lídrov na trhu*** **,** Presentation at PosAm SECURITY Day, PosAm, s.r.o, Bratislava, 27.VI.2006. *http://videoarchiv.posam.sk/*

[1] **Semančík, R.:** ***Enterprise Digital Identity Architecture Roadmap*** **,** Version 1.2, Technical White Paper, nLight, s.r.o, Bratislava, 2005. *http://www.nlight.sk/documents/enterprise-digital-identity-architecture-roadmap-v1-2.pdf*

[2] ***Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*** **,** Official Journal of the European Communities L 13, 2000.

[3] ***Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such dat*** **,** Official Journal of the European Communities L 281, 1995.

[4] ***Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation*** **,** Liberty Alliance Project, 2005. https://www.projectliberty.org/specs/Circles_of_Trust_Legal_Framework_White_Paper_322200522576.pdf

[5] **Semančík, R.:** ***Choosing the Best Identity Management Technology for Your Business*****,** Technical White Paper, nLight, s.r.o, Bratislava, 2006. *http://http://www.nlight.sk/documents/2006-infosecon-contribution-final.pdf*

PosAm