# CHOOSING THE BEST IDENTITY MANAGEMENT TECHNOLOGY FOR YOUR BUSINESS

Ing. Radovan Semančík
IT Architect
nLight, s.r.o.
Súľovská 34, Bratislava, Slovakia
+421 2 43642084, Fax: +421 2 43642086, E-mail: semancik@nlight.sk

**Abstract.** This paper summarizes the motivation for deploying identity management technologies and their features. The three areas of identity management are described: enterprise identity management, user-centric digital identity and government identity management. The specific problems of these areas are discussed together with possible solutions. The identity problems that span all three areas are described at the end of the document. The document concludes by summarizing the current state of identity management technology.

## INTRODUCTION

The Internet changed everything. It changed the application architecture, it has changed the way how we communicate and co-operate, and even more changes can be expected in the next few years. But there is still one aspect of computer systems that works the same way from the ancient times of computing: identity management.

The identity management has started as set of manual processes to create, modify and delete user records in computer systems and partly has also covered user authentication. But the growth of Internet and the distributed nature of current applications make the manual processes infeasible.

New concepts and technologies were introduced to address the identity management problems. These technologies has started in three different environment that suffer from a specific set of problems: enterprise, Internet and government. According to this, there are three basic areas of identity management technologies:

- **Enterprise Digital Identity** aims to automate user management processes in the enterprise environment, such as user **provisioning** process, user repository management, authentication, authorization, etc.

- **User-Centric Digital Identity** is a set of concepts that may provide mechanisms for management of user's data in the Internet environment.
- **Government Digital Identity** focuses on management of data that describe physical persons. The data managed by government usually forms the legal aspects of the person's lives.

While the approach to solve the identity management problems may be different, all the identity management technologies have many common aspects. The specifics as well as common features of these technologies are described in the following sections.

## ENTERPRISE DIGITAL IDENTITY

Information systems in the enterprise have very complicated character and heterogenous structure. While the “business” features of these systems are usually integrated, the integration of infrastructure components is not very common. The user management, as an infrastructure service, is usually implemented separately in each system and the user administration is done manually by a team of system administrators. This approach brings many problems, such as high operational cost, difficult auditing, inconsistent user databases, slow reaction to security incidents, and many others.

Several mechanisms were proposed to address these problems, each mechanism solving different set of problems or taking a different approach. While there is a lot of different technologies, only two of them gained wider acceptance and only these two are discussed in the paper (for the full description of enterprise identity management technologies see [1]). The two major enterprise identity technologies are described bellow:

- **Directory Services** provide a unified repository of user data. The most common access protocol is Lightweight Directory Access Protocol (LDAP), which provides standard method for accessing the directory. Directory services usually provide relatively tight-coupled integration of user databases. For example the applications need to agree on a common user identifier, attribute names and meanings, etc. Some related technologies allow to translate data between several directory services (meta-directories) or provide a unified view of these services (virtual directories).
- **User Provisioning Systems** automate user management tasks. The provisioning systems do not aim to create a single user database. These systems instead try to manage the flow of changes in the different databases and replicate these changes to end systems as necessary. For example, when new employee is hired a new record describing the employee appears in the HR system. The provisioning system detects that, determines a correct role for the employee and creates accounts in information

systems as needed. Provisioning systems are usually workflow-based, very flexible and allow integration of several systems in loose-coupled fashion.

The heterogenerity of information systems in the common medium-to-large enterprise environment makes it nearly impossible to implement single directory system directly for the following reasons:

- **Lack of a single, coherent source of information.** There are usually several sources of information for a single user. For example HR system is authoritative for the existence of a user in the enterprise and for assignment of employee identifier. The Management Information System is responsible for determination of user's roles (e.g. in project-oriented organizational structure). The inventory management system is responsible for assigning telephone number to the user. The groupware system is authoritative source of the user's e-mail address and other electronic contact data. There are usually 3 to 20 systems that provide authoritative information for a single user.
- **Need for a local user database.** Some systems must store the copies of user records in local databases to operate efficiently. For example large billing systems cannot work efficiently with external data. Legacy systems usually cannot access the external data at all (e.g. do not support LDAP protocol).
- **Stateful services.** Some services need to keep state for each user to operate. For example file servers usually create home directories for users. While the automation of state creation can usually be done on-demand (e.g. at first user log-on), the modification and deletion of state is much more difficult.
- **Inconsistent policies.** The role names and access control attributes may not have the same meaning in all systems. Different systems usually have different authorization algorithms that are not mutually compatible. While this issue can be solved with per-application access control attributes, the maintenance of these attributes may not be trivial. A complex tool for transformation and maintenance of access control attributes (usually roles) may be needed.

Even using meta-directory or virtual directory mechanisms may not provide expected results, as such systems only provide the data and protocol transformation, but do not change the basic principle of directory services. A more complex approach is needed to manage the user‘s records in heterogeneous systems, especially in large enterprise environment. User provisioning systems are usually well-equipped for these complex tasks. Complex transformations, approvals and correlations can be implemented by workflow engines in user’s provisioning systems. But user’s provisioning systems exhibit their own problems:

- **Slow operation.** The workflow processes directed from the information source towards the end systems are usually triggered asynchronously and therefore can immediately react to a change. But the execution of a workflow process itself can take considerable amount of time, especially if user interaction (approval) is required. The processes that synchronize data in the opposite direction – from the end systems towards the provisioning system – are usually not triggered asynchronously. The synchronization of changes in this direction may take several hours or days. The provisioning systems are designed to handle the complexity and are not designed for high performance. Single operations exhibit high latency and low throughput, bulk operations are limited to basic operations only.
- **Risk of inconsistency.** The provisioning systems synchronize several data repositories. The repositories may become temporarily inconsistent, if the provisioning system does not detect the change immediately. The data may even become permanently inconsistent, due to the problem occurring in synchronization processes.

It can be seen that both the directory services and the provisioning systems need to be deployed in the enterprise environment to address the identity management problems. We propose high-level architecture for enterprise identity management that contains both directory services and provisioning systems (Figure 1). We assume that the primary sources of  data relevant for an assembling user identity are various enterprise information systems (e.g. HR or MIS systems). In the proposed architecture, the user provisioning system will synchronize the data from various sources and provisions to unified view of data to the central enterprise directory service. The directory service may act directly as the user repository for stateless systems and services. The directory may also provide a repository for the enterprise authentication mechanisms or  the Single Sign-On system. The provisioning system will also manage user's records in stateful and hybrid (partially stateful) systems, but these systems may also use authentication services and/or directory service directly. Legacy systems can only be managed by the provisioning system, as these usually cannot effectively adapt to the change of authentication or  the user repository mechanisms. A virtual directory system may be deployed in addition to the provisioning system. The use of virtual directory may streamline the data synchronization, but will likely not negate the need for a provisioning system.

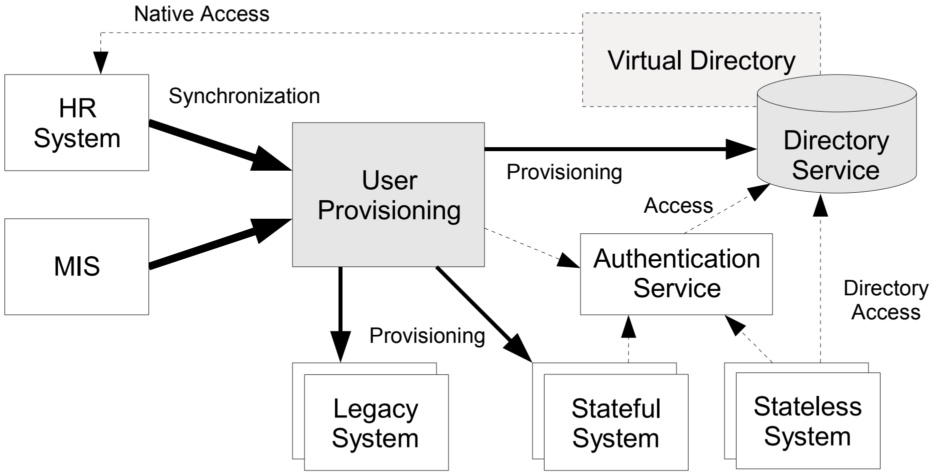

**Figure 1**

The directory services will likely evolve beyond the simple concept of current LDAP-based servers. The simple static attributes may be replaced by the dynamic attributes or service pointers to provide location information, calendar services and other dynamic data.

The enterprise environment is no longer as isolated as it used to be in the past. The enterprises are more open, co-operating with other organizations, such as the partners, the suppliers and the customers. The enterprise information systems must adapt to this change to be effective, and so must the identity management technologies. As the information systems in two enterprises are not under the same organizational control, the mechanisms described above cannot be directly used for cross-organization identity management. The identity management system that aims to provide interoperability between businesses must be both loose-coupled and standard-based.

**Identity Federation** is a mechanism, that focus*es* directly on the cross-domain identity management. The basic principle of the identity federation is an exchange of identity claims (or assertions) between interested parties. Such claim may state that a user from one organization is already logged-in in the local enterprise information system and therefore should have direct access to the partner's organization resources (Figure 2). The claims may also contain attributes stating user's characteristics such as full name or department. But the attributes may also be used for asserting that the user belongs to a specific group or a role, that can be used for the access control.

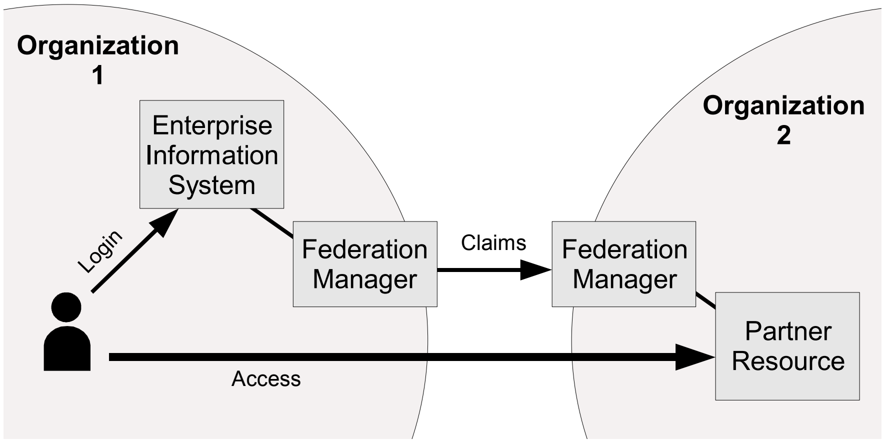

**Figure 2**

The identity federation technology is not limited to “federating” organization employees. It was also designed for integrating customer’s experience between different sites. This aspect of identity federation technology falls into the user-centric identity area, described bellow.

## USER-CENTRIC DIGITAL IDENTITY

The Internet protocols were designed without special attention to security and privacy, which is a cause of frequent problems. Various forms of electronic fraud (“phraud”, [2]) have begun to spread through the Internet, that are difficult to fight with the use of traditional methods [3]. The many forms of automated Internet misuse (such as “spam”) hints that a major change in basic Internet security and privacy mechanisms are needed. The major identity-related problems of the current Internet environment can be summarized as:

- **Traditional authentication.** Majority of Internet sites use static passwords for authentication. This mechanism is not only weak, but it is also uni-directional. User authenticates to the server, but the server is not authenticated to the client. Using HTTPS protocol with server authentication may not be a sufficient solution [3]. In addition to this, the common Internet user has to remember tens or even hundreds of credential sets (user’s name/password), which leads to “credential overload”. Users are compelled to use the same credentials on several sites or to store credentials in insecure storage.
- **Personal data out of control.** Personal data are spread through the Internet with minimal subject's control over them. The plethora of registration forms makes it difficult for users to remember what data was submitted to what site. Once the data is submitted, it is difficult to take it back (to revoke it). Privacy policies and privacy notices are incomprehensible for an average user. Users are not in control of their personal data.

- **Obsolete application architecture.** Majority of the current web-based systems supports only the simple data models to describe users. Usually these models only contain simple, local and static attributes, that cannot be easily extended. The web applications cannot adapt to distributed and dynamic attributes such as the location data, the scheduling ( the calendars) or the reputation. The complete redesign of the application is required to adapt to new Internet paradigms.

Several systems were recently introduced to address these problems [4]. Table 1 describes the basic properties of the selected Internet identity systems. These systems claim to provide mechanisms for reliable transfer of the personal data between Internet sites. The data is accompanied by security tokens, that maintain data integrity and provide source authentication.

| System | Security Token | Identifiers | Origin |
|---|---|---|---|
| Liberty | SAML | Pair-wise random (local) | Liberty Alliance Project |
| WS-Federation | Username, X.509, REL, SAML | Not specified | BEA, IBM, Microsoft, RSA Security, Verisign |
| LID, LID 2.0 | GPG signature | URL | NetMesh |
| SXIP 1.0 | XML digital signature (non-standard) | GUPI (global) | SXIP Identity |
| I-Name SSO | SAML | XRI | XDI.org |
| Digital Credentials | Digital Credentials | Not specified | Credentica |
| OpenID | SHA1, Diffie-Hellman (non-standard) | URL | OpenID.net |

**Table 1**

All user-centric identity systems are still under development, none of them providing a complete solution. Each system adopts different approach and therefore these systems are in most cases non-compatible. A solution called the “Identity Selector” was proposed by Microsoft [5], to address the compatibility issues and also to partially improve the workstation security problem.

## GOVERNMENT DIGITAL IDENTITY

The representation of physical person in the digital world has attracted public attention only recently. The first identity-related technical topic that has paid governmental attention was a concept of digital signature. The digital signature mechanism was codified in Europe by the Directive 1999/93/EC [6], which was applied to EU local legislation. The directive specifies only the mechanism for digital signature creation and validity, it does not specify the framework for person identification and the personal data management. Such framework was partially set by the Directive 95/46/EC [7], that specifies the rules concerning the personal data transfer and processing. None of the directives specify the mechanisms in sufficient details; therefore each country is implementing the systems differently [8]. This inconsistency impacts especially the user-facing interface of the government systems, which may prove problematic in the future.

The internal government information systems are usually heterogeneous, administered by different departments and are not well integrated. The personal data may be inconsistent or incorrect when seen in cross-system context. The situation in the government information systems area is similar to that of the large enterprise systems. Therefore the methods and tools used for the identity management in government may be similar to those implemented in enterprise identity management projects. This approach will at the very minimum help to address in internal inconsistency and integration of government information systems.

On the other end of the government systems spectrum is so-called e-government identity, which is focused on communication with citizens using electronic channels. The prominent technology in this area used to be X.509-based public key infrastructure, but that may not be desirable in the future. The current practice of certificate authorities is to assign the unique identifier to each physical person for relatively long period of time (usually one year). Whenever the person presents the certificate, the person's privacy is likely to be compromised. Therefore the X.509 certificates are practically limited to communication between citizens and the government. Other methods may be needed for general citizen-to-business communication, management and protection of personal data. It may be expected that the methods described in the user-centric identity section will assume this role in the future.

## COMMON PROBLEMS

Almost all described identity management technologies suffer from a set of common problems. These problems are mostly caused by  the legacy architectural approach and the lack of security and privacy features in current technologies. The most severe current problems may be summarized as:

- **Global identifiers.** Many systems use global identifiers to identify users, such as Social Security Numbers, URLs or e-mail addresses. Global identifiers 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 [9]. Viruses and other malware can easily infect the workstation and gain control over all user's activities. While the workstation is under malware control, user's activity can easily be tracked, entered passwords can be observed and even complex man-in-the-middle attacks against strong authentication mechanisms could be

mounted. Many government digital signature schemes can also be subverted using client-side malware.

- **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.

While some technologies address some aspects of these problems, no complete solution exists. Global identifiers can be replaced by local, pair-wise identifiers, but this approach usually suffers from honeypot effect on the identifier repository. The workstation security problems can only be satisfactory solved by the complete redesigning of a client operating environment [9], possibly also by the introduction of the hardware security support.

## CONCLUSION

The mosaic of the identity technologies is far from being finished. While the technologies in the enterprise identity management area are effective and can deliver a value, other areas are not that advanced. The Internet, user-centric identity technologies are in early development stages and have many interdependencies on other technology areas. The consumer’s expectations, the needs and the full implications of “identity paradigm shift” has to be understood before final solution can be deployed. The government identity technologies are based on legacy mechanism that does not adapt well to the specifics of information age. The correct approach has to be determined slowly, gathering experience in small steps.

## REFERENCES

[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] Felten, E., W., Balfanz, D., Dean, D., Wallach, D., S.: *Web spoofing: An internet con game*, Proceedings of 20th National Information Systems Security Conference, Baltimore, 1997.

[3] Emigh, A.: *Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures*, Radix Labs, 2005. *http://www.antiphishing.org/Phishing-dhs-report.pdf*

[4] Semančík, R.: *Internet Single Sign-On Systems*, In: Bieliková, M. (Ed.): Proceedings of IIT.SRC 2005: Student Research Conference in Informatics and Information Technologies, Bratislava, Slovakia, pp. 116-123, 2005.

[5] *Microsoft's Vision for an Identity Metasystem,* White Paper, Microsoft, 2005. http://www.identityblog.com/stories/2005/10/06/IdentityMetasystem.pdf

[6] *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.

[7] *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 data*, Official Journal of the European Communities L 281, 1995.

[8] *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

[9] Brunnstein, K.: *About Inherent Insecurity of Contemporary ICT Systems, and about Future Safety and Security Requirements*, Proceedings of Information Security Summit, Prague, 2002.