Communications of the Association for Information Systems

Volume 25 | Number 1 Article 42

12-1-2009

Tutorial: Identity Management Systems and Secured Access Control

Anat Hovav
Korea University Business School, anatzh@korea.ac.kr

Ron Berger
Seoul National University

Recommended Citation

Hovav, Anat and Berger, Ron (2009) "Tutorial: Identity Management Systems and Secured Access Control," *Communications of the Association for Information Systems*: Vol. 25, Article 42.
Available at: http://aisel.aisnet.org/cais/vol25/iss1/42

Communications of the Association for Information Systems

CAIS

Tutorial: Identity Management Systems and Secured Access Control

Anat Hovav

Korea University Business School

anatzh@korea.ac.kr

Ron Berger

Seoul National University

Abstract:

Identity Management has been a serious problem since the establishment of the Internet. Yet little progress has been made toward an acceptable solution. Early Identity Management Systems (IdMS) were designed to control access to resources and match capabilities with people in well-defined situations, Today's computing environment involves a variety of user and machine centric forms of digital identities and fuzzy organizational boundaries. With the advent of inter-organizational systems, social networks, e-commerce, m-commerce, service oriented computing, and automated agents, the characteristics of IdMS face a large number of technical and social challenges. The first part of the tutorial describes the history and conceptualization of IdMS, current trends and proposed paradigms, identity lifecycle, implementation challenges and social issues. The second part addresses standards, industry initiatives, and vendor solutions. We conclude that there is disconnect between the need for a universal, seamless, transparent IdMS and current proposed standards and vendor solutions.

Keywords: Identity management systems, information security, access control

Volume 25, Article 42, pp. 531-570, December 2009

I. INTRODUCTION

The word *identity* dates back to 1570[1] and is defined by the Merriam-Webster dictionary as "the distinguishing character or personality of an individual." Dictionary.com offers a broader definition: "the condition of being oneself or itself, and not another."[2] By adding the word itself, the definition includes persons and objects. Both definitions highlight the fact that an identity is used to separate one entity from all others. Wikipedia defines *digital identity* as "the digital representation of a set of claims made by one digital subject about it or another digital subject."[3] A digital subject may be human using a digital device (computer, PDA, mobile phone) or nonhuman, such as devices and computers requesting services of one another. Thus:

> ***A digital identity represents a set of unique, distinguishing digital characteristics or claims that could establish the identity of the subject, that is, ensures that the subject is who or what it claims to be.***

In the physical world, humans use a number of identifying tools:

1. Things they know, such as their name, address, age, social security number, or items that are verifiable against physical records such as a social security card, a driver license, or a passport
2. Things they carry, such as an idcard or a credit card
3. Things they are, such as their height, weight, and hair and eye color

During a transaction between two subjects, one uses their five senses to verify the claims of the other (e.g., visual, audio). Therefore, when a customer purchases a product at a physical store, the clerk can visually verify the credit card, compare the signature, and often the picture id-card. This ability to use our trusted senses to verify the claims of a subject creates trust between the two transacting entities.[4] In cyber space, as stated by Peter Steiners's cartoon, "... nobody knows you're a dog" [Steiner 1993]. Thus, digital identities deal with the complexities of replacing simple human abilities with complex systems that attempt to mimic human intuition. One of the key issues facing society is that, with the advent of the Internet, we are more dependent on eLife[5]; functions that as recent as ten to fifteen years ago were completed in the physical space now occur in cyber space (e.g., commerce, financial, government transactions, communication). However, rather than develop separate logical identities for cyberspace, our "physical identities" became a de facto standard for our digital identities. That is, most websites require identifying elements that we traditionally use in the physical world, such as name, credit card numbers, address, and phone number. This state of affairs introduces two major challenges:

1. Security. Computers and networks are susceptible to hacking. Once hackers obtain a digital identity they can use it in the physical world, resulting in identity theft.
2. Privacy. The ability to map one's digital identity to a physical identity creates major privacy concerns. This is especially true due to the large number of databases containing private information such as health care, financial, and marketing.

In the early 2000s, industry, governments, policymakers, and casual computer users became aware of the risk involved in the use of physical identity components in cyber space. Awareness led to attempts to develop standards, frameworks, and implementations of IdM systems in which digital entities are provisioned based on strong technical authentication tools. These topics are discussed in the following sections.

[1] http://www.merriam-webster.com/dictionary/identity (last accessed 08/16/2009).
[2] http://dictionary.reference.com/browse/identity (last accessed 08/16/2009).
[3] http://en.wikipedia.org/wiki/Digital_identity (last accessed 08/16/2009).
[4] Even here, fake and/or forged identities can be used by people trying to outwit the other party.
[5] eLife refers to portions of our lives that occur in cyber space from communicating with others (e.g., e-mail) to commerce, entertainment (internet TV), and web 2.0.

II. CONCEPTUALIZATION OF CYBER IDENTITY

Although the concept of a digital identity is not new, the terminology used to describe it and its association to Identity Management is not well defined. The discussion in this section is mostly drawn from a document maintained by Pfitzmann and Hansen [2006] last revised in May 2006. The basic assumption of this discussion is that communication among entities or subjects is done by sending and receiving messages over a communications network. This assumption is in line with most client/server, Internet, or SOA architectures, and thus we feel that it is not unreasonable. In addition, we assume that some level of anonymity is a desired state for senders and receivers.

Anonymity is defined as the inability to identify an entity. Anonymity ensures that a user may use a resource without disclosing its own identity. Anonymity also assumes that it is not possible to link a resource or a message to a particular sender (*sender anonymity*) or receiver (*receiver anonymity*), nor that a pair of sender/receiver is linked (*relationship anonymity*). Ultimate (or strong) anonymity may be a desirable state. However, full anonymity prevents useful communications. For example, if an anonymous sender sends a message requesting a web page, the receiver (web server in this case) must be able to link the request to an IP address, a domain name and a port number to reply, thus reducing anonymity. Therefore, Pfitzmann and Hansen [2006] introduce the term *pseudonymity*. As will become clear later, pseudonymity could be equated with digital identity. A *pseudonym (or a nym)* is an identifier of a subject (sender, receiver, entity), other than its real name. The holder of the pseudonym is the user (regardless if the pseudonym was chosen by the user or was randomly created by the system). A pseudonym may be linked to a single user or a group and can vary over time. The existence of a pseudonym does not guarantee anonymity.

Authentication and Accountability[6]

Unlike in the physical (face-to-face) world, in cyber space, identifying and authenticating are not synonymous. While identifying establishes the unique characteristics of a subject, authenticating verifies, or validates that identity. Therefore, authentication depends on the ability to link a pseudonym to an entity. This ability is important to achieve accountability. For example, a user-id and password establishes the identity of the subject using them. However, if a user discloses her user-id and password to a co-worker and the co-worker uses the identity to enter the system, the system identifies a subject but validates or authenticates the wrong identity.

The need to verify the claims of a pseudonym introduces the concept of *identity broker*. Identity brokers are trusted third parties (other than the sender or receiver) that adhere to certain rules[7] and maintain the link between the pseudonym and the identity of the user. Identity brokers reveal the linkage when and if necessary. The ability of identity brokers to link pseudonyms to actual identities is an essential component of accountability. To achieve accountability, it should be possible to authenticate and certify an entity. That is, the identity broker should certify the original identity of the pseudonym holder. The transfer of such authentication (or other attributes of an entity) by a third party is also termed *credentials.* The term *credential* is used often in the IdMS literature. In general, anonymity and accountability are two extremes of the privacy continuum. Anonymity (i.e., the inability to link a message to its source) ensures complete privacy, while accountability requires some level of disclosure. The concept of pseudonymity allows implementing a compromise solution between accountability and anonymity. To increase anonymity, a system might use a chain of identity brokers.

Types of Pseudonyms

Pseudonyms vary in their strength (i.e., their ability to hide the link to the “real identity”). For a *public pseudonym,* the link between the pseudonym and the holder are public knowledge (such as a phone number of a person or an IP address of a server). For an *initial non-public pseudonym*, the link between the pseudonym and the holder is accessible but not publicly known. Often identity certification authorities (or identity brokers) hold that information. In the case of an *initially unlinked pseudonym*, the link is (initially) unknown. For example, the link between biometric attribute and a given user (e.g., eye retina signature) is unknown, unless the user records it somewhere.

Pseudonyms also vary depending on who holds them. A *person’s pseudonym* is a replacement for the person’s true identity (i.e., physical identity). A *role pseudonym* is limited to a specific role (such as a customer using an e-commerce website). A person might have many roles (see Figure 5), and a role might be held by several persons. Pfitzmann and Hansen [2006] define a *relationship pseudonym* and a *role-relationships pseudonym* to denote the pseudonym used to communicate with a given partner and a given role. For example, a person might communicate with a website in her role as a vendor while at work and as a customer otherwise. Occasionally, systems create

[6] Although Pfitzmann and Hansen do not assert that authentication is a requirement for a pseudonym’s link to a real identity, others do (for example, see Darmiani, De Capitani di Vimercati, and Samarati 2003).

[7] What is considered an “acceptable set of rules” is a technical and social issue and will be discussed later.

transaction specific pseudonyms, which are only valid for the duration of a given transaction (e.g., fund transfer systems). A person's pseudonym is considered the least anonymous while a transaction pseudonym is the most anonymous.

An example of a mechanism to implement pseudonyms is PKI (public Key Infrastructure) where public key certificates and digital signatures are issued by certificate authorities to ensure the identity of a user while maintaining a "reasonable" level of anonymity and accountability.

Roles, Partial Identities, and Digital Identities

In the context of identity management, the concept of an entity or subject can refer to a person, a machine, or a program. If one of the ultimate objectives of an IdMS is to maintain the privacy of an entity, it is logical to confine the discussion to human actors. Yet, most of the current literature defines entities in the global sense and only occasionally refers specifically to humans. An *identity* is defined as a set of attributes that uniquely identify an entity. Because an entity might have various roles, depending on the situation, the context and with whom they communicate, an entity is, therefore, likely to have a number of *partial identities,* each containing some of the attributes of the complete identity. A pseudonym is said to identify a partial identity.

A *digital identity* is defined as (identifying) attributes that are accessible by technical means (i.e., that can be stored and retrieved by computer-based systems). For example, a digital identity may be an e-mail address or a user name. Although the term *virtual identity* appears in the literature, it is used most often in reference to virtual worlds (i.e., games) and rarely used in the context of IdMS.

Identity Management, Privacy, Reputation

Identity management refers to the process of managing partial identities and pseudonyms. It includes the design and administration of attributes and pseudonyms to be used. An identity management system enhances *privacy* if it limits the linkage between the pseudonym and the partial identity by selecting "proper" attributes. Privacy-enhancing applications follow the "need to know" rule, that is, messages between sender and receiver and the attributes of the pseudonyms used do not provide more linkage to the partial identity than is necessary to achieve the objectives of the application. When re-using a partial identity, the user can build a *reputation* (positive or negative). For example, an e-mail address that is used repeatedly to send e-mail messages will find its way to the INBOX (i.e., good reputation); while an e-mail address from certain regions known for spam (based on country code) is likely to find its way to the SPAM box (i.e., bad reputation). Much like other systems, an identity management system does not need to be computer based. People often manage their partial identities and pseudonyms off-line (a phone book, a list of credit card numbers, PINs). In this tutorial, we refer to Identity Management Systems (IdMS) as computer-based systems that design and administer (partial) identities, pseudonyms, and their attributes. IdMS refer to the architecture required to support identity management applications, by which users manage their partial identities, communication, privacy, and security. A more detailed discussion of the characteristics of IdMS is presented in Sections V and VI.

The goal of this paper is to describe some of the contemporary computer-based approaches to the management of digital identities given the above conceptualization of identity, anonymity, accountability, and privacy. We begin with a historical overview of digital access control and the challenges they present, followed by the characteristics of IdMS, technical and conceptual components of IdMS, technical challenges, social challenges, proposed standards and standardization organizations, and vendor implementations.

III. HISTORICAL OVERVIEW

In the early days of computing, computer systems were monolithic and relatively isolated from the external environment. During the mainframe era, accessibility was controlled by physical means. That is, computers were locked in specialized rooms, and access to data and information was limited to printouts and physical reports, and dumb terminals. Access control was a relatively simple mechanism, since all dumb terminals had to be connected to the processor (CPU) via a control unit (CU). This type of connection applied to local terminals (directly connected to the CU) or to remote terminals (connected via dial-up networks and modems). This architecture was based on a static port allocation. The CU identified terminals based on their physical location and address. Remote terminals could not connect directly to the processor and had to have a static callback phone number to be a legitimate user. Thus, users' identification and privileges were based on the physical location/connection of the terminal they used.

For example, the initial version of IBM's RACF (Resource Access Control Facility) authenticated terminals based on their physical address.[8]

As multitasking increased and with the advent of local area networks (LAN), more granular and dynamic access control became necessary. The next phase was the implementation of the traditional user-id and password combination (also known as logical access control). Logical access controls rely on Access Control Lists (ACL) and one of three elements:

1. What you know
2. What you have
3. What you are

First Generation AC—What You Know

The oldest, simplest, and cheapest form of access control relies on a key word, phrase, or combination of characters selected by the user and known only to the user. The system identifies the user based on the proper combination of an id, a password, and sometimes a pass phrase. The assumption is that a correct combination of these elements authenticates the user and provides her with proper privileges. However, first generation ACL suffers from the following limitations:

1. Simple or short passwords are easy to break using brute force attacks or dictionary attacks (Table 1). Thus, users are required to create long (8 or more characters) and unintuitive passwords.
2. To avoid possible attacks, passwords need to be replaced regularly, increasing users' resistance and frustrations.
3. Users are susceptible to social engineering and tend to share their user-id and passwords with co-workers, friends, and figures of authority [Cazier and Botelh 2007].
4. Most users have several user-ids and passwords creating a password overload syndrome.[9] A study by RSA found that 28 percent of corporate workers juggle 13 or more passwords while 30 percent of workers rely on 6 to 12 passwords.[10]
5. As a result of password overload, users tend to:
   a. Select easy to remember passwords, which are easier to break
   b. Write their passwords and keep the notes in obvious locations such as under their keyboard, behind their screen or on their desk
   c. Record their passwords on their PDA, cell phones, or in a file on their desktop
   d. Require additional support from helpdesk personnel, increasing organizational costs. It is estimated that the cost to resolve a password problem by helpdesk personnel cost from $10 to $31 per inquiry [Kho 2009]

[8] In 1976 IBM introduced RACF (Resource Access Control Facility) as an add-on layer to their mainframe operating system. RACF has been upgraded as IBM introduced new versions of its operating system and used as the main security component of IBM mainframes for the last 30+ years (http://www.sans.org/reading_room/whitepapers/mainframes/a_return_to_legacy_security_247?show=247.php&cat=mainframes). (last accessed 08/16/2009).

[9] http://www.net-security.org/article.php?id=750 (last accessed 08/16/2009).

[10] http://www.informationweek.com/news/global-cio/showArticle.jhtml?articleID=171201187 (last accessed 08/16/2009).

Table 1. Estimated Time to Break a Password. Adapted from Whitman and Mattord [2005]

Number of Characters in Password	Estimated time to Break—All Lower Case	Estimated time to Break—Upper Case Used
4	2.7 seconds	9.5 seconds
5	3 minutes and 2 seconds	15 minutes, 17 seconds
6	3 hours, 26 minutes	23 hours, 57 minutes, 14 seconds
7	9 days, 17 hours, 26 minutes	3 months, 3 days, 19 hours
8	1 year, 10 months, 1 day	24 years, 6 months

Second Generation AC—What You Have

As organizations began to implement client-server architecture, dynamic remote access, and Intranets and Extranets, the need for additional layers of secure accessibility became apparent. Security was especially important for the financial and health industries due to increasing privacy related regulations (e.g., HIPAA). Second Generation access control mechanisms incorporate an additional layer. The user is required to have a physical component (e.g., card, key, token) to gain access to the system. After the user enters her user-id and password, she will use the physical component to confirm her identity. Some systems use a key (much like a door key) while some systems use synchronized tokens (Figure 1).

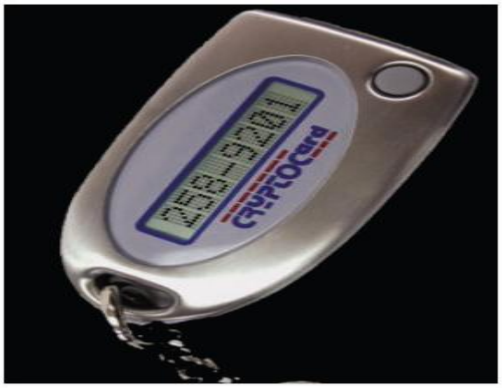


Figure 1. An Access Control Token[11]

Second Generation access control alleviate some of the issues discussed above. For example, if hackers break the user-id and password, they cannot gain access to the system unless they can access the “token.” Remote social engineering is also impossible. User-ids and passwords could be replaced less often, since today’s advanced tokens are dynamic and provide the added security necessary. However, other issues (overload, using familiar words, recording the passwords) remain a challenge for security managers. More so, internal sharing and internal social engineering continue to be a problem, since users who share passwords will also share their token.

In addition, users are required to deal with an added layer of security, which entails additional work and increases users’ resistance. Users also tend to forget, misplace, or lose their tokens requiring additional help and costs such as the cost to disable and replace the lost token, the costs of temporary tokens, and the cost to reset the system. For example, a physician goes on vacation, and, thinking that he will not need access to patients’ records, he leaves his token at home or in his office. An emergency occurs, and the physician's specialized skills are needed. Since the physician, cannot access the system without the token, the system administrator has to be summoned to reset the system, disable the token, and allow temporary remote access without the token. Although the above is a rare example, similar scenarios increase users’ frustrations.

[11] http://www.cryptocard.com/uploads/Documents/DataSheets/DSKT120071211A4.pdf (last accessed 09/07/2009).

Third Generation AC—What You Are

With the advent of the Internet and e-commerce, organizations started to face additional challenges. First, they had to protect not only their own machines, but somehow ensure that personal computers used by online customers are also protected. Second, collaboration among websites requires the ability to transfer users' identity. In addition, e-commerce increases the exposure of personal data. In the past, most organizational data was internal. With e-commerce, organizations started to accumulate large amounts of consumers' private information. Thus, the need for increased security, privacy, and protection of users' financial information (credit cards, bank accounts, and Social Security numbers), and medical information resulted in organizations adding another layer of access control. Third-generation AC relies on one or more biological features of the user. Biometric mechanisms include many technologies. The simplest and cheapest are fingerprinting and voice recognition. These two techniques are easy to implement and often rely on hardware already embedded in most Personal Computers (such as a microphone) or on relatively cheap enhanced equipment (mouse or fingerprinting keyboard—Figures 2 and 3).

Figure 2. Finger Printing Mouse

Figure 3. Finger Printing Keyboard

The disadvantage of the fingerprinting and voice recognition techniques is that they are relatively easy to forge and are not reliable, especially in a highly noisy environment (for the voice) or a dirty environment (for the fingerprinting). Other biometrics techniques include hand and face geometry, palm scans, retina and iris scans. Each of the techniques has its benefits and challenges and works best at certain environments and for certain applications. Biometrics are ranked based on their type I and type II error rates, ease to forge, level of intrusiveness to the user, required environmental conditions, and cost (cost to implement, space and processing requirements, availability of equipment). For example, an iris scan, which is the most reliable technique, is intrusive and expensive to implement. Biometrics offer an additional layer that can ensure that the user identified is indeed the proper one (authentication). However, beyond the limitations of cost and intrusiveness, biometric controls are limited to human actors and would not work for bots or web services. In addition, it is difficult to implement biometrics outside organizational boundaries. For example, it might be prudent for an online bank to require some level of biometric identification from its online customers. However, the bank risks customer resistance to the added cost and a resulting loss of market share because of lack of flexibility, fear, or technical limitations. Assuming, a customer wants to access her account away from her home computer, she would have to find a computer equipped with the proper biometric device. Unless all hardware providers and banks agree on a universal standard configuration that includes certain biometric devices and banks provide these devices at little or no cost, mandating the use of biometrics may not be "good business."

IV. CURRENT STATE OF AFFAIRS: THE "SILO" APPROACH

In recent years, the term *identity management* replaced the term *access control.* This new term indicates the need to verify the identity of the entity accessing the system and the negotiation of rights and privileges based on privacy requirements associated with that identity. Identity management architecture could be server-based, client-based, or networked-based [Kock and Worndl 2001]. At present, the most common architecture is proprietary, application driven, and server-based. For example, amazon.com and facebook.com each maintains its own users' information. This results in a "silo" approach, as illustrated in Figure 4. That is, a user often has many digital identities, each is managed by a different entity and requiring its own resources.

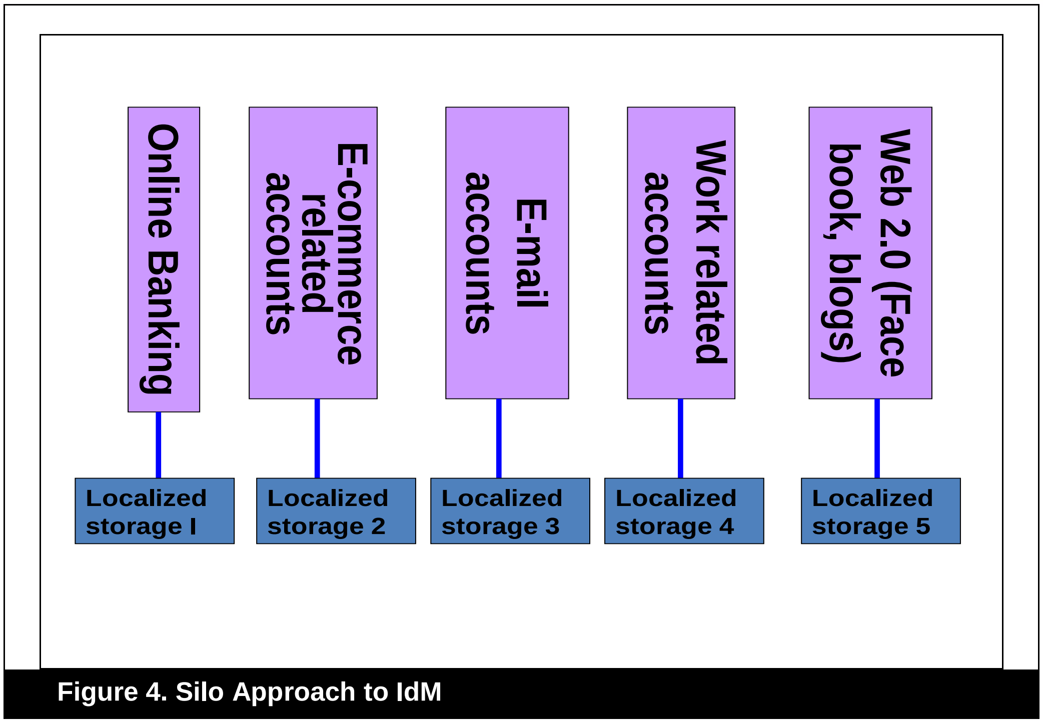


Figure 4. Silo Approach to IdM

A limitation of the silo, server-based approach is that a user must manage a large number of identities. In addition, users do not control the maintenance of their identities, privacy requirements, or related attributes.

For example, Appendix A illustrates the differing requirements of IdMS in three domains: healthcare, which is regulated; e-learning, which is relatively open to allow freedom of expression; and e-government, which is highly secure to prevent cyber-terror incidents. A user is often a stakeholder in more than one domain and, therefore, is likely to maintain a number of partial identities, each with different privacy requirements. In our example, a person might be a patient with high privacy requirements. The same person could also be involved in e-learning or e-teaching, requiring another partial identity (with relatively low privacy requirements) and is most likely engaged in some e-government activities (e.g., e-filing of income tax) requiring a highly protected partial identity. In today’s society, users are involved in a variety of online activities and access a large number of applications in various geographical locations (Figure 5).

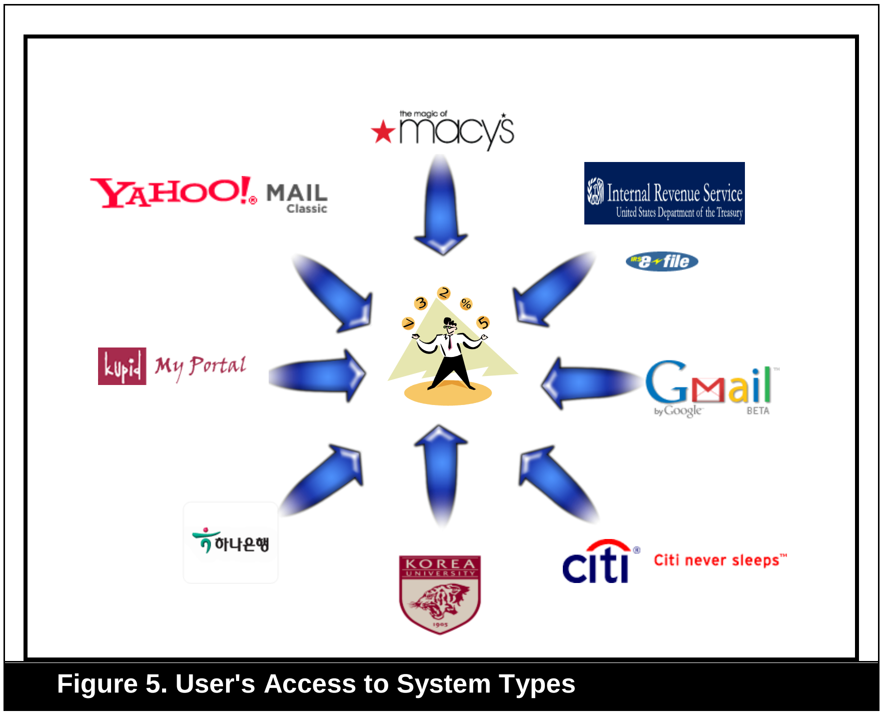


Figure 5. User's Access to System Types

In summary, today’s identity management “silo” approach does not align well with most users’ diverse and dispersed activities. In addition, this approach does not support web services, ad-hoc and mobile computing, and has the following limitations:

1. It mostly relies on physical identity elements. Thus, an exploitation of a cyber identity could result in impersonation in the physical world.
2. It is relatively easy to break. Attackers can link pseudonyms to real identities.
3. It is centralized within an application. For each application, the provisioning, maintenance, and management are done by that service with little transferability to other services.
4. Users have to log-on to several systems, creating overhead and loss of productivity.
5. It lacks federation. Each application uses its own scheme, standards, and requirements in providing authentication and permissions.
6. It is inefficient, expensive, and does not align with current business trends (Figure 5).
7. It is organizational centric rather than user-controlled. Users have minimal control over their privacy.
8. Users juggle a large number of identities, each related to a set of application type. These identities are not integrated or standardized.
9. It lacks support for nomadic, wireless, peer-to-peer, and ad-hoc architectures. Since most current IdM are server-based, they require the existence of a centralized, static processor.
10. The current lack of universal standards and governance results in:
    a. Inconsistencies in implementations across organizations and technologies
    b. Lack of universal metrics that measure levels of security of a given application or system
    c. Various systems have different levels of security resulting in inconsistencies. Thus, a very secure system may become vulnerable by being associated with a less secure system.
11. Lack of seamless interoperability among systems.

Starting in the mid 1990s, a number of companies, consortia, and standardizing organizations attempted to create a universal framework for the management of cyber identities**.** Most notable are the centralized approach introduced by Microsoft (i.e. Passport), the federated approach introduced by the Organization for the Advancement of Structured Information Standards (OASIS) and the Liberty Alliance project, and most recently the user-centric approach initially developed by Korea’s Electronics and Telecommunications Research Institute (ETRI) and later adopted by the ITU. These and other frameworks are described in detail in Section IX. Each of the approaches uses slightly different terminology and is based on a slightly different paradigm. The centralized (Passport) approach is rarely used and thus is not discussed further. The federated and user-centric approaches will be discussed in Sections IX and X. In the remaining sections of the paper, we integrate the concepts and terminology used by each of the approaches.

V. CHARACTERISTICS OF IDENTITY MANAGEMENT SYSTEMS

A person’s physical identity begins when they are born (our name, lineage) and lasts until they pass on. However, over their lifetime, people may use a number of *logical identities*. For example, at work, one is identified based on such factors as their position in the organization, job title, skills, and employee id-number. The same person is identified based on their social security number and financial portfolio (accounts, investments, loans) by their bank. Similarly, a *digital identity* might take many forms. An entity might have several partial identities depending on their cyber activities. As mentioned above, an identity contains three components: identifier, authenticator, and privileges. Identity management defines and manages the life-cycle and profiles of digital identities, and the exchange of information necessary to validate and authorize these identities.

Principles of IdMS

To overcome some of the limitations in current IdMS, several research groups, policy makers, and industry leaders are proposing frameworks for the deployment of IdMS. In this section, we describe several conceptual frameworks. In Sections IX through XI, we discuss several global standards currently under development and vendors' implementations.

Table 2. Principles of Identity Management Systems [Cameron 2005]

Principle	Description	Comments
One	User consent	An identity is identified and used only when the user agrees to it.
Two	Limited disclosure	The system provides the minimum identifying information required for the transaction.
Three	Fewest parties	Only parties that "need to know" receive identifying information.
Four	Directional identity	Omni-directional versus uni-directional[12]
Five	IdMS should work with a variety of identity technologies, run by multiple providers.	Designers cannot assume the feasibility of a universal identity or the availability of a single expression of an identity.
Six	Human integration	High levels of reliability between the human user and the system
Seven	Consistent experience across platforms	Similar to the way the web appears to users

Cameron [2005] suggests seven principles that should drive the development of IdMS (Table 2). The core of the principles is the idea that IdMS should be an encapsulation or a meta-protocol much like the Internet Protocol (IP) or the hypertext protocol (HTTP). IP for example, does not care what device is attached to the network, which operating system is run, the speed of the network or packaging of the message. As long as the payload (data) is packaged in IP compatible packets, transmission over the Internet is achievable. Similar claims can be made about HTTP. Conceptually, an IdMS should behave the same way. That is, regardless of the format or content of the digital identity, each device attached to the network should be able to process it.

The seven principles in Table 2 (also known as the *"The laws of identity")* describe a conceptual framework of a meta-IdMS that drives Microsoft's implementation of their Digital IdWallet product (see Section X). The framework also introduces some technical and social challenges. Most notable, who is to decide what is the "minimum required" and who defines "need to know." We address these challenges in Section VIII.

Desired Characteristics

One of the key elements of IdMS is that they will be user-driven (or user-centric). IdMS should be easy to use and maintain even by novice computer users. Users should be able to create and revoke partial identities as they see fit, based on a set of negotiated and agreed-upon privacy rules. Users should also be able to maintain their own profiles. Ideally, the process of provisioning, maintaining, and revoking identities should be as automated as possible.

In addition, IdMS should have at least the following characteristics:[13]

1. Adaptive. The identity and its management should adapt to changing requirements and system conditions.
2. Universally accessible. Users access systems from a variety of locations. An IdMS should support a user regardless of their physical location, level of connectivity, or protocol used.

[12] Omni-directional refers to a public identity that is known and accessible to all (such as a universal web-service, or an RFID tag). Uni-directional refers to a private identity that is established between the service provider and the user.

[13] Primarily based on a report by the national science and technology council subcommittee on biometrics and identity management published in Sept 2008 http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf (last accessed 09/03/2009).

3. Extensible in space. Allows growing numbers of applications, attributes, and scope (activities).
4. Cross-domain integration. Allows applications in various domains to communicate and share users' provisions.
5. Cross-technology integration. Allows access from a variety of devices.
6. Federated support and distributed management. The ability to integrate partial information to form an identity from multiple locations and applications, and certification authorities.
    a. Single sign on and sign out. Users should be able to use one point of entry (authentication) to access a federation of services.
7. In line with current social norms of privacy and in compliance with basic regulatory frameworks. This requirement is challenging and is discussed in detail in Section VIII.
8. Allow minimal risk of exploitation, change, theft, unauthorized transfer, and all other potential misuse. Identifiable information is released only when and if required by the transaction.
9. Support accountability, non-repudiation, and audit-ability. All parties to a transaction should be responsible and accountable for the consequences of that transaction. Audit and forensic capabilities are needed to track, investigate, and resolve misuse and other disputes.
10. Viability. Financially viable for organizations.
11. Support a minimal level of trust. From a technical perspective, a set of minimal standards required to authenticate a user and the assurance that one application can provide another as to the security level of that user. From a social perspective, trust relates to agreed-upon voluntary governance. The issue of trust is discussed further in Sections VI and VIII.
12. Reputation model. Provides the users with the ability to build reputation over time.

VI. COMPONENTS OF IDMS

At present, IdMS frameworks could be characterized by their approach and the type of user they support (Table 3). IdMS frameworks are based on the existence of a federated certificate provided by an entity that authenticates the user or service, or a token the user (or service) holds. Table 3 describes the prevalent standards and implementations. Additional details are given in Section X and Appendix B. In the discussion in this section, we include components from all implementations. Often, various implementations have a different name for the same technical component. We highlight the parallels when possible.

Table 3. The Four Paradigms of IdMS

	User	Web Services
Federated	OASIS/Liberty	Oasis/Liberty
Token	ITU-T	WS-*

- *Digital identity repository.* IdMS often use a digital identity repository that contains policies and meta-directories to govern access. In addition, an application privileges system contains information about entitlement to resources, information, and access. These repositories may reside on various machines and physical locations. They might be implemented on a variety of hardware and software solutions and use a number of configurations. The *discovery process* is used by the provider to locate relevant authentication and authority data across distributed domains and systems. *Digital identity stores* is a term used by Microsoft to describe a repository of digital identities.

- *Identity provider (IdP).* The IdP links the subject (user, entity) to its given identity, authenticates the subject and provides a certificate or a token, which enables other components to recognize the subject. The identification and authentication process uses a variety of mechanisms and strengths depending on the requirements of the given application.

- *Relying party/service provider.* The services that rely on the credentials provided by the IdP are called *relying parties.* They are also known as *Service Providers* (SP) since they provide the services requested by the user. Service providers have to decide if they accept the assertions provided to them by the IdP for a given request from a particular entity. The term *identity federation* is used to denote a trust relationship between the SP and the IdP. An identity federation between the two providers exists when the SP accepts assertions about an entity from the IdP.

- *Authentication and certification process.* This process certifies the data—the recipient of the data has the ability to validate and verify its authenticity. A *claim* is an assertion that certain identifying information such as a name or a credit card truly belongs to a given digital entity. Claims could be an *identifier* (such as a user name) or an *attribute* (such as a user age or gender). The terms claims and assertions are used in the Microsoft sphere. These terms are equated with pseudonyms, partial identities, and linkability in the Open Standards sphere.

  The actual implementation of the authentication process varies depending on the standard. For example, Microsoft's CardSpace uses an InfoCard as a way to identify entities to the relying party. In the Liberty Alliance model, a user/ entity authenticates once to the service provider using one of its partial identities and can then access any service in the provider's "circle of trust." The identity provider is the only entity in the system that should be able to link a pseudonym to its original owner and thus is accountable for any misrepresentation or dispute.

- *Identity providers and notary.* Often the communicating parties are unknown to each other and, therefore, cannot trust that the identities are properly authenticated. This can occur in ad-hoc or peer-to-peer communications. A third party trusted vendor could be employed to authenticate identities and their assertion. This is often referred to as a *federated notary* [Goodrich et al. 2008].

- *Credentials.* "A credential is an attestation of qualification, competence, or authority issued to an individual by a third party with a relevant *de jure* or *de facto* authority or assumed competence to do so." Examples of credentials include academic diplomas, security clearances, identification documents, badges, passwords, user names, keys, and powers of attorney.[14]

  The system determines a set of rules as to who could read, modify, or access a given credential. There are several types of credentials: *raw credentials*, are specified by the user or other entity, without any guarantee to their validity, *authenticated credentials* are digitally authenticated by the user or an issuing party but are not validated, and *validate credentials*, are guaranteed by a credential broker. *Credential issuers* or brokers are third-party trusted entities that issue validated credentials.[15] Credential brokers might collect credentials from a variety of sources. To be trustworthy, credentials should have the following characteristics: unique, verifiable, issued by a broker with good standing, and governed.

- *Identity syntax and attributes.* An Identity profile should contain several user attributes and credentials. Such attributes might be personal data, habits, and biometrics. Different standards and implementations use different structures to describe attributes and credentials. Ideally, those should be interoperable.

- *Policy control.* Policy control governs access to information and determines how information is used, disclosed, audited, and logged. Rather than proprietary, application or operating system driven access control, IdMS purport integrative policies to govern access. Policy controls use *policy sets*, a collection of policies, rules, obligations, and a target. The control uses predetermine algorithms to combine rules. *A rule* specifies permission (or a denial) to perform an action on an asset. *A target* is a set of conditions and actions that must be met for a policy to apply. Organizations' security policies are complex and contain thousands of rules. Often policies that affect a particular digital asset are written from a variety of views and are difficult to integrate.[16] Languages such as XACML (Extensible Access Control Markup Language) enable developers to combine all the policies that affect a request (for service, or asset) into one integrative policy. Policy controls may also generate alerts, when information is accessed.

[14] http://en.wikipedia.org/wiki/Credentials (last accessed 08/16/2009).

[15] It is possible that the IdP will also act as a credential broker but not necessary.

[16] For example, request to access a mail sever could be handled by a system-specific policy that determined the configuration of a firewall (that is the firewall is configured to allow access to the server from any IP address but only through ports 25 and 80). Alternatively, it could be handled by an issue-specific policy that deals with users' accounts and rights.

- *Provisioning.* Companies enable users' access to certain digital assets (e.g., networks, applications, devices such as a PDA, or credit cards). The process of rationing assets to employees is termed *provisioning*. While the term *provisioning* is often used in reference to employees, organizations also provision assets to other stakeholders, such as temporary employees, consultants, customers, and suppliers. *Provisioning mechanism* refers to the automation of the workflow of systems, devices, services, and other resources to various stakeholders. For example, as a temporary employee logs into a system, they are provisioned access to certain resources and services depending on their role and tasks. At the end of their engagement, the system de-provisions these resources. Similarly, a web service might be provisioned access to a particular data store for the duration of a request.

- *Token.* As mentioned above, some standards and implementations use the concept of a token. A token contains claims (or assertions) about the entity requesting the service (the requestor) and may be codified using a variety of structures (for example, WS-* uses the concept of token and can seamlessly interoperate with other tokens regardless of the structure they use). A *Security Token Service* (STS) and related protocols are used to request or issue the token (i.e., WS-Trust), while a related set of policies describe the STS and its associated claims (i.e., WS-SecurityPolicy).

Technical Aspects of a Universal Trust Model

Applications rely on the identity assertion established by the identity provider. There has to be a certain level of trust between the application and the provider. That level of trust varies depending on the subject, its roles, the applications' level of security and the privileges provided to the subject. A global trust model is required to support a universally accepted identity management system. Such a model requires accepted standards and metrics. For example, a credit card transaction in country X will receive assertion from the provider associated with the card issuer residing in country Y. The various stakeholders (i.e., cardholder, merchant, issuing bank, clearing house, Credit Card Company) are likely to have separate systems and reside in different physical locations. Yet, typically, they all agree on what constitutes a legitimate credit card transaction for the particular card used and the particular holder, and what level of assertion is required to accomplish such a transaction. Conceptually a universal digital identity should work the same. Establishing a certain set of global requirements, standards, and metrics are an integral part of a universal trust model. The Liberty Alliance "circle of trust" has 150 members with 400 million Liberty-enabled identities and clients, while a token approach assumes that possession of a token implies trust. However, at present (in 2009), we see a large number of "islands of trust" rather than a universal trust system.

Identity Life-Cycle

The traditional identity lifecycle is sequential, starting at the origination of a digital identity through its maintenance and, finally, termination. A digital identity life-cycle contains the following stages:[17]

- *Establish the identity by linking the pseudonym to an entity's information.* For example, a user might establish a user's name and password, which is linked to a bank account, a credit card, and other financial information.

- *Re-establish the identity.* A second pseudonym may be linked to the same information (i.e., another service is using the credit card to complete a purchase), or pseudonym is linked to additional information.

- *Describe the identity by assigning it attributes.* These attributes may be specific to a certain entity or service.

- *Maintenance.* Over time, the various attributes assigned to an identity are likely to change.

- *Audits.* Log and record the activities of an identity and allow user access to the log for verification purposes.

- *Analysis.* Analyze patterns of an identity's behavior. Analysis enables the system to create base-line behavior patterns and alerts when behavior deviates from the established baseline.

- *Terminate the identity when necessary.* Disassociate the pseudonym from the entity.

However, this sequential approach is insufficient when dealing with multiple identities for a given object at any given time. Dimiani et al. [2003] suggest that provisioning of identities should be automated. That is, users should be able to automatically obtain and create identities allowing easy and fast access to information resources. This approach is applicable mostly in the web environment or inter-organizational settings. In intra-organizational settings, auto-provisioning reduces user reliance on helpdesk and is more cost effective. Automated provisioning must comply with

[17] http://en.wikipedia.org/wiki/Identity_management_systems (last accessed 08/16/2009).

organizational policies. Thus, when a user creates an identity, her privileges are limited to information and resources applicable to her role, rights, and needs.

Revocation should also be automated. When an employee leaves a company, all her provisions are revoked automatically. Automated revocation and synchronization of all relevant accounts is a technical and an organizational challenge. For example, an employee of Intel gave two weeks notice before leaving for a job with a competitor. Based on organizational policies, his privileges remained the same for the two weeks between his notice and departure. The employee downloaded a large number of confidential documents depicting future chip designs. Intel sued the employee. In his defense, the employee claimed that he acted within the bounds of the law, since at the time he downloaded the documents he had legal access to that information. At the time of the lawsuit, the employee did not sell the information or share it with anyone and thus was within his legal rights.[18] This case exemplifies the complexity involved in auto-revocation of authority. Organizations must decide at what stage of the separation process an authority is revoked. An alternative concept is *partial* or *gradual revocation* in which organizational policies trigger reduction in privileges when an employee announces his intended separation.

More generally, when an employee changes location, position, or role, the IdMS should automatically change the employee's provisions. This process is easier to implement if proper communication exists between Human Resources and the Information Security function.

In summary, user-driven, policy control identity management life cycle is heavily depended on strong organizational policies and their clear implementation both at a technical level (automated provisioning and revocation) and at the organizational level (communicating changes in rights, assignments, and rules).

VII. TECHNICAL CHALLENGES

Despite notable advances achieved in the development of IdM concepts, standards, and implementations, a number of technical challenges remain to be solved. Some of the technical issues are being researched and can be resolved with additional technological developments, while other issues may be more complex and will require universal agreements.

- *Proliferation of dormant identities.* As discussed in Section IV, profile management of a digital identity should be user-driven, limiting the users' reliance on the helpdesk. However, systems should be able to limit the proliferation of unused identities, and the number of identities created by users. Often when users forget their identifying information (id, password), it is easier for them to create a new identity with slightly different parameters than to ask helpdesk for the original information (or a reset). It is difficult for websites (especially e-commerce sites) to keep track of duplicate partial identities. A proliferation of rarely used identities increases hacking risks[19] and waste of resources. At the same time, the decision when to archive or purge a partial identity when dealing with external entities (such as an e-commerce website's management of casual buyers) must be managed cautiously. Deleting a dormant identity may result in the loss of a potential customer. Organizations should decide whether the risk of losing a potential customer exceeds the risk of maintaining a large number of dormant identities. For example, I use Travelocity.com because they already have my profile and I can complete a transaction quickly and efficiently. However, occasionally, my account remains dormant for six months or even a year. Upon returning, I expect to be able to use my old account and my old profile. If I find that my identity was removed and I have to re-provision, I am likely to try a competing site.

- *Where should the various components be located?* A server-based IdM results in a "silo" approach and depends on the existence of a central processor (Section IV). A client-based IdM enables users to manage and control their identities and is not application dependent. However, inasmuch as users use a variety of clients (e.g., a desktop at home or work, laptops, PDA, smart phones), they would need to implement a version of their IdM on each client. A third alternative is a distributed system. However, distributed IdM presents additional challenges of interoperability and compatibility across systems.

- *Automated lifecycle.* The idea of an automated lifecycle (specifically provisioning and revocation) could be implemented for intra-organizational systems where the boundaries are clear. Users are provisioned access when they work for the company (e.g., as a permanent employee, consultant, vendor) and are revoked when their engagement is over. However, when the relationships between the service and the user are ad-hoc, automated provisioning is more difficult to implement.

[18] http://www.thetechherald.com/article.php/200838/2027/AMD-employee-charged-with-stealing-trade-secrets-from-Intel (last accessed 08/16/2009).

[19] Hackers often use dormant accounts when breaking into systems.

- *Representation.* Another technical challenge is the representation of a digital identity and the best format in which to exchange attributes and assertions between resources. This is especially a challenge when a digital entity requires access to a number of partner systems, each running on a different architecture, network, operating system and each with its own set of requirements. Dimiani et al. [2003] suggests identity ontology and a metadata describing the entity. However, the syntax for profiles should reveal the minimal disclosure required to complete a transaction.

- *Interoperability.* When creating digital identities, organizations often collect data from a variety of sources. This may lead to interoperability issues. This challenge is augmented by the current lack of an interoperable, universal standard. In addition, the number of attributes for an entity can depend on who defined the identity. IdMS should be able to consolidate these definitions and create an interoperable meta-definition that is recognized by all participating asset providers. Often a user is identified by one source, but the transaction requires the involvement of several partnering organizations. Although the originating partner provisions the entity, the remaining partners should be able to determine their own level of trust. For example, a user enters a system via a portal and provides a user-id and password, which is deemed sufficient to browse certain e-commerce sites. However, when the user is ready to purchase an item, the e-commerce website (who the user is accessing through the portal) might or might not feel that the user-id and password are sufficient to verify the user's ability to pay for the purchase. The site is likely to require additional information, such as a credit card, a PayPal account, or a bank account number. Ideally, an IdMS should contain enough metadata to eliminate such interoperability challenges.

- *Consolidate attributes.* Similarly, an IdMS should be able to consolidate attributes and other relevant pieces of information regarding the user's identity that are stored in various places and are accessible in various contexts. Continuing the Travelocity example above, assuming that a user accesses a car rental website through the Travelocity portal, the car rental company uses Travelocity.com's initial identity provisioning to "trust" the inquiry. In addition, when ready to make the car reservation, the car rental company, needs a form of payment guarantee and information regarding the user's driving credentials. On the other hand, if a user purchases a flight ticket, the airline company is interested in different information. Presently, users provide such information manually and separately. Ideally, an IdMS should be able to determine the context and needs of each partnering organization and provide enough information to generate a trusted transaction, but not more.

- *Single point of failure.* The reliance on a single sign on or a central IdP could potentially create a virtual single point of failure. Any failure of that service could cause the entire system to collapse. A failure could be the result of a hacking attack, a compromise of the policy repository, a physical cause (e.g., power failure) or any other technical problem that would compromise the service integrity or availability.

- *Balancing between linkability for accountability purposes and privacy.* User driven IdMS should enable users to decide which identity they want to use and which attributes and credentials they want to release when conducting a particular transaction. However, for the sake of accountability, some linking to private (or identifiable) information is required, endangering privacy. At present, the ability to provide accountability without exposing some level of private information (to potential attackers) remains a challenge. Similarly, IdMS should link just "the right amount" of information needed to complete the transaction. Cameron [2005] terms it "minimal disclosure" (see Table 2). However, deciding how much information is "just enough" could be a challenge when managing a large and dynamic number of entities, identities, and credentials. Papastergiou et al. [2007] proposed a framework for privacy-enhancing IdMS with high levels of minimization. The proposed model allows users to make an informed decision regarding their pseudonyms and partial identities. Users can control which personal data is linked to a given partial identity. Although this proposal is a potential solution to the linkability problem, it relies on users' technical sophistication and security awareness. This issue is discussed further in Section VIII.

- *Reputation building model.* Presently, most reputation-building models are based on the number of times an entity accessed a resource or service. Gaining "reputation" could improve the performance of the system and the services provided to users. However, attackers can use these algorithms to increase their reputation artificially until they gain enough credentials to launch an attack. This approach is similar to what happened to eBay, where a group of social engineers conducted "legitimate" transactions (buying and selling) among themselves, increasing their ratings over time.[20] Once they had high ratings, they started posting fictitious expensive products for sale. They received the money but never sent the items to the buyers. Subsequently, eBay established escrow services for expensive items. The same scenario could occur in the domain of identity reputation. However, creating "escrows" for identity credentials is more complex.

[20] http://news.cnet.com/2100-1017-238489.html&tag=mncol%3btxt (last accessed 09/12/2009).

- *Performance*. Strong encryption and complicated access control policies could cause the system performance to deteriorate. Occasionally, requirements are relaxed to accommodate for performance. For example, under Kerberos, a SOAP message is accompanied by a ticket. Due to performance considerations, only the first message contains the ticket. Following messages contain a KeyIdentifier—a hash value of the ticket. With the increase in network and processor speed and the development of special security appliances, performance issues will decrease.

- *Possible attacks.* Finally, computer scientists and researchers are discovering various possible attacks against published standards. For example, Cervesato et al. [2007] described a man-in-the-middle attack that can breach the authentication guarantees of Kerberos. Sidharth and Liu [2007] described several potential attacks against web services that could be used to compromise identities and their authentication. Alrodham and Mitchell [2007] illustrated two possible vulnerabilities in CardSpace,[21] an identity management system used by Microsoft.

VIII. SOCIAL CHALLENGES

In addition to the technical challenges discussed in Section VII, the development of universal identity management systems faces major social challenges.

Trust

One of the challenges facing eLife is the lack of trust by users. As the number of cyber attacks and identity thefts increases, it will be more difficult to convince users to trust technology. IdMS, as a new technology, face several similar trust issues.

- *Users' trust of the system.* Users should be able to trust the various components and agents involved in setting their identities, linking private information to pseudonyms, and provisioning resources. Users should also be able to audit these agents and verify the information and credentials they provide others.

- *Trust among service and identity providers.* Although, some "circle of trust" include a large number of participants and stakeholders, not all of them could be "trusted." Recent cases of security attacks against credit card processors and other financial companies, and the exposure of private data, creates doubt in their ability to secure data stores. Yet the core concept of federated and distributed identities depends on the ability of any service (also termed *relying service)* to trust the credentials provided to them by other entities.

- *Trust among agents and services that originate from participating countries.* Due to lack of a central governing body and a universal set of laws, trust is limited to agents and services that originate from participating countries. However, it is relatively easy for hackers in non-cooperating countries to circumvent messages and "pretend" to be a trustworthy provider, agent, or service. This subterfuge can result in a greater lack of trust among participants.

Privacy Issues

One of the desired characteristics of IdMS is to be in-line with current social norms and privacy requirements. However, the concept of privacy varies by individual, society, and culture. Privacy is defined differently in different countries. For example, South Korea requires all bloggers to register their real name and identity number (equivalent to social security number) before being able to post messages online. For residents of the U.S., such a request is considered an invasion of privacy. In April 2009, the Korean government asked Google.com to adapt their system (i.e., require the registration of real identities) for users that upload videos to YouTube or cease operation in Korea. Initially, the company stated they would eliminate uploading capabilities in Korea. However, as of July 2009, Google.com executives are debating between discontinuing their presence in Korea or requiring the disclosure of users' real name and number from any video upload originating in Korea.[22] This example illustrates the difficulties in creating a universal identity management system that would accommodate privacy needs of all countries and cultures.

In addition, balancing between accountability and privacy is a challenge. The basic idea of IdMS is to increase privacy by assigning pseudonyms to entities. However, to ensure audit capabilities and non-repudiation, identity providers have to maintain a link between the pseudonym and the entity, limiting users' privacy. An attack on the identity providers' systems may result in the exposure of millions of links and user private information.[23]

[21] For more information on CardSpace see http://msdn.microsoft.com/en-us/windows/aa663320.aspx (last accessed 09/01/2009).
[22] http://english.hani.co.kr/arti/english_edition/e_business/304002.html.
[23] At the Blackhat conference (2009), Kaminski, a well known hacker, described how to trick a certificate authority into providing a certificate to an unqualified entity (http://news.cnet.com/8301-27080_3-10299459-245.html?tag=mncol;txt).

Global Reach or a Digital Divide?

The Internet's global reach creates social issues related to Identity management. Differing information security laws among countries provide "safe heavens" for hackers. Countries with limited privacy and security laws are known as hotbeds for hacking attacks. Hackers could potentially use social engineering methods to set fake identities and build trust over time. Once those identities are trusted, they can be used to extract information and access secure websites.

Another challenge related to universality is the potential creation of a digital divide. Many of the standards used to implement federated identities are based on the concept of "circle of trust." Circles of trust are industry, services, or even country based (i.e., the Shibboleth project in the U.K.)[24] and thus result in a number of "islands of trust." Federated identities could provide great benefits to the companies in the circle and draw users to these websites. However, many third-world counties might be excluded due to their unfavorable legal environments, lack of compliance, or poor infrastructure. Organizations in these countries might be prevented from joining the circle of trust resulting in loss of potential improvements in their Internet environment, leading to the reversal of current efforts to introduce technology and the Internet to underdeveloped countries. In addition, the membership in the circle has to be maintained over time. As new technology is introduced and as hackers develop new attacks, companies in the circle need to upgrade their systems in a timely manner.[25] The "circle" has to appoint an objective and independent entity to inspect members periodically and ensure that they continue to comply with existing and new standards. Rules of removal and reinstatement of members must be universally acceptable.

Finally, since there is no universal governing body that regulates the Internet, disputes over IdMS and repudiation of transactions could not be easily resolved. Identity and credential brokers do not and could not have global jurisdiction. That is, credentials provided by a broker in one country may not be accepted in a disputed litigation in a court of another country.

Users' Awareness and Training

User centric IdMS require users' awareness and training. For example, the concept of "minimum data" is based on the idea that users decide what information should be disclosed to an entity and who "needs to know." Similarly, the concept of maintaining a client-based token requires some understanding of what it is and what should be done to keep it safe. These decisions require users to understand the various types of information, their privacy level, rules, and policies of websites they access and determine a basic set of rules that best work for them. At present, most users have limited understanding of these issues. In addition, social engineers pry on users' naiveté regarding information security and identity management, resulting in increased identity theft incidents.

Even within organizations, end-users are rarely trained enough to comply with organizational information security policies. This problem intensifies when dealing with non-organizational users (e.g., elderly, less educated). Who would be responsible for the training and awareness of users, and what methods are best to achieve such massive training remains to be seen.

Identity Management or Big Brother

Although technically, federated identity does not mean "one identity fits all," conceptually the loss of one access mechanism could open the door to many websites. At present, many breaches are the result of users' mistakes or social engineering attacks. For example, as stated in Section III, users tend to share their passwords if they believe that the asking entity is in a position of authority, a friend, or someone in need [Cazier and Botelho 2007]. Presently, due to the "silo" approach, if a user reveals her user-id and password (intentionally or not), a hacker could gain access to one or two websites at most. With federated IdM, access to one's user-id could potentially open access to the person's entire portfolio. Thus, although federated identity could improve access management, it could also increase risk. Hackers will gain more financially[26] by getting a person's identity information and are likely to increase their efforts to obtain such information. Given that most such information is stored at the IdP, these systems are likely to become an obvious target for hacking attacks. Similarly, in countries where the government controls access to the Internet, the existence of a federated IdM could increase government control over users and limit free access to resources.

[24] http://en.wikipedia.org/wiki/Shibboleth.
[25] What constitute "timely" has to be decided by the standards organizations and participating members.
[26] The market value of an identity increases as the number of websites it accesses increases.

IX. STANDARD SETTING ORGANIZATIONS

In the preceding sections, we introduced the proposed conceptualization and frameworks of IdMS and some of the socio-technical challenges involved in the implementation of such systems. In the following sections, we detail existing standards and vendor implementations, and compare the conceptual frameworks to these implementations. We find that, at present, several standards setting organizations operate in the IdMS arena and although their proposed standards contain some common components and building blocks, the standards remain isolated. Thus, we conclude that without convergence, the future of IdMS is in question. These standards address two main areas:

1. User driven access to the web and other resources
2. Web services accessibility

The Microsoft's approach (adopted by the ITU-T) and the OASIS/Liberty approach (Appendix B) differ substantively. Microsoft IdM provides a token that the user can use to access any website. This approach is similar to a key that opens many but not all doors. Once the entity receives the key from the identity provider (gatekeeper), it can open X number of doors, depending on the key. Once inside the room, the entity could engage in various activities (gain access to various assets), depending on the room and the type of key it has. The ITU-T standard is user-driven. It enables the user to access any resource that accepts the key regardless of location or affiliation. However, it also depends on the users' ability to maintain the security and confidentiality of the key.

Liberty IdM authenticates a partial identity of an entity once, and then the identity is free to use all services that are part of a given circle of trust. The Liberty approach is similar to a person given access to a large hall by the guard. Once inside, the person can use any facility in the hall. Its presence in a particular "circle of trust" is enough to grant it access to services. This approach assumes a central authority within each circle and results in potentially many "islands."

OASIS[27]

The Organization for the Advancement of Structured Information Standards (OASIS) was initially formed in 1993 as the Standard Generalized Markup (SGML Open), and is presently a global consortium. OASIS promotes the development and adoption of e-business and web standards such as web services, e-commerce, security, law and government, supply chain, and computing management. In 1998, the high tech industry shifted to XML. As a result, SGML Open converted from SGML to XML and changed its name to OASIS. Also, the focus of the consortium shifted from promoting adoption to developing technical specifications. In 1999 OASIS was approached by The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), a committee of the United Nations dealing with standards for business, to jointly develop a new set of specifications for electronic business. Initially, OASIS had five technical committees; by 2004 there were seventy.

Specific standards related to IdM developed or adopted by OASIS include:

- SAML—Security Assertion Makeup Language, a standard XML-based framework for the secure exchange of authentication and authorization data. OASIS approved SAML v. 1.0 as a standard in November 2002 and SAML v. 1.1 in August 2003. OASIS approved SAML v. 2.0 as a Committee Draft in December 2004 and as a standard in early 2005.

- SPML—Service Provisioning Markup Language, a standard XML-based framework for the secure exchange and interoperation of service provisioning requests. OASIS approved SPML v. 1.0 as a standard in November 2003.

- XACML—eXtensible Access Control Markup Language, a standard XML-based protocol for access control policies. XACML is a method for conveying biometric identity data such as retina scans and fingerprints. OASIS approved XACML v. 1.0 as a standard in February 2003, approved v. 1.1 in August 2003, and v. 2.0 in September 2004.

- WS-Security—Web Services Security, a standard method for attaching security data to a web services message. OASIS approved WS-Security v. 1.0 as a Standard in April 2004.

Some argue that the liscensing restrictions posed by OASIS render their standard as not open and hinder universal adoption. This topic is beyond the scope of this paper.

[27] http://en.wikipedia.org/wiki/OASIS (last accessed 08/16/2009).

Liberty Alliance

Liberty alliance was formed in 2001 and is a consortium of sixteen companies representing a variety of industry leaders such as Sun Microsystems, AOL, American Express, Nokia, and Entrust. The organization presently has over 150 members, including governments, and educational institutions. A members list can be found at http://www projectliberty.org/liberty/membership/.

According to the project website, there are more than 400 million Liberty-enabled identities and clients globally. In addition, hundreds of companies and organizations participate in the various special interest groups (SIGs) and activities. Their goal is to develop open source standards and best practices for the implementation of IdMS. Enabling devices and identities of all types to be linked by federation and protected by universal authentication. As of 2009, The Liberty Alliance project had tracked over a billion identities and devices using one or more of their standards.

Figure 6 describes the general Liberty model developed by Cameron and Jones [2006], using a single sign-on. A "principal" or user federates various identities to a single identity issued by an IdP. The user can access services provided by Service Providers (SPs) within the same circle of trust by authenticating once to the IdP. Access relies on a pre-established trust relationship between the IdP and every SP in the circle of trust. In Figure 6, the user has federated its identities within the circle of trust A and circle of trust B.

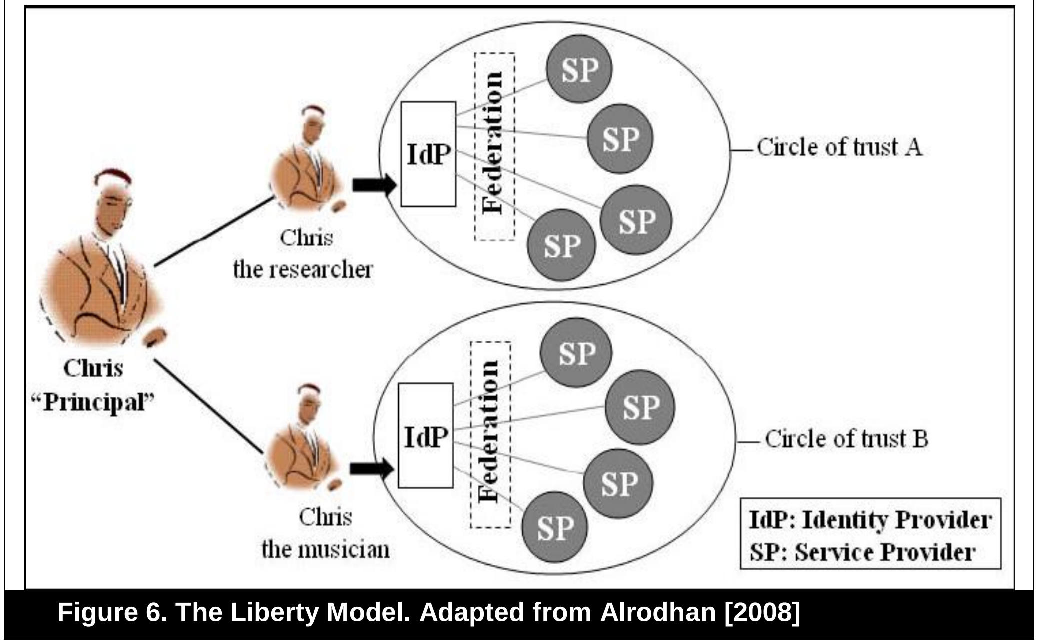


Figure 6. The Liberty Model. Adapted from Alrodhan [2008]

Figure 7 describes the architecture proposed by Liberty. The Liberty implementation specifications are divided into three frameworks: the Identity Federation Framework (ID-FF) [Watson 2009], the Identity Web Services Framework (ID-WSF) [Tourzan and Koga 2009] and the Service Interface Specifications (ID-SIS) [Kellomaki 2003]. These frameworks are discussed in more detail in Section X.

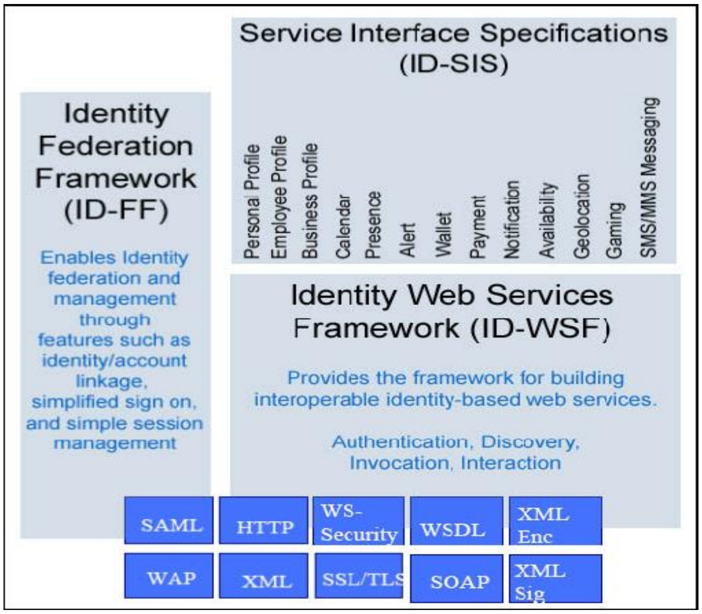

Service Interface Specifications (ID-SIS)
Personal Profile
Employee Profile
Business Profile
Calendar
Presence
Alert
Wallet
Payment
Notification
Availability
Geolocation
Gaming
SMS/MMS Messaging
Identity Federation Framework (ID-FF)
Enables Identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management
Identity Web Services Framework (ID-WSF)
Provides the framework for building interoperable identity-based web services.
Authentication, Discovery, Invocation, Interaction
SAML
HTTP
WS-Security
WSDL
XML Enc
WAP
XML
SSL/TLS
SOAP
XML Sig

Figure 7. The Liberty Frameworks. Adapted from Alrodhan [2008]

ID-FF Liberty profile types include Single Sign-On and Federation Profiles, Register Name Identifier Profiles, Identity Federation Termination Notification Profiles, Single Logout Profiles, Identity Provider Introduction, Name Identifier Mapping Profile, and Name Identifier Encryption Profile.

ITU and ITU-T[28]

The International Telecommunication Union (ITU) was founded as the International Telegraph Union in Paris in May 1865. It was established to standardize and regulate international radio and telecommunications. The ITU main responsibilities include standardization, allocation of radio spectrum, and organizing interconnection arrangements among countries for international phone calls. The ITU is a specialized agency of the United Nations, and its recommended standards carry a high degree of international recognition compared with other organizations that publish technical specifications.

The ITU contains three sectors:[29]

- Telecommunications Standardization Sector (ITU-T): Secretariat is the Telecommunication Standardization Bureau (TSB), known prior to 1992 as the International Telephone and Telegraph Consultative Committee (CCITT).
- Radiocommunication Sector (ITU-R): Secretariat is the Radiocommunication Bureau (BR), known prior to 1992 as the International Radio Consultative Committee (CCIR).
- Telecommunication Development Sector (ITU-D): Secretariat is the Telecommunication Development Bureau (BDT), created in 1992.

The ITU is an intergovernmental public-private partnership and as of 2009 has 191 countries in its membership, 700 public and private sector companies, and international and regional telecommunication divisions.

ITU-T[30]

The ITU-T coordinates and ensures efficient and timely standards for all areas of telecommunications for the ITU. The international standards proposed by the ITU-T are referred to as "recommendations." They become mandatory only when they are adopted as part of a national law for a given country. As the Internet and the web became

[28] http://en.wikipedia.org/wiki/ITU (last accessed 08/16/2009).
[29] http://www.itu.int/ITU-T/50/docs/ITU-T_50.pdf (last accessed 08/16/2009).
[30] http://en.wikipedia.org/wiki/ITU-T (last accessed 08/16/2009).

prevalent, the ITU decided to rename the International Telephone and Telegraph Consultative Committee (CCITT) to Telecommunications Standardization Sector (ITU-T). This change in name broadened the scope of the committee to include networks and other telecommunication areas.

The ITU-T publishes new and updated "recommendations" regularly. As of 2009, it has over 3,270 "recommendations" in their library. Also, the ITU-T facilitates the cooperation with other standards developing organizations (SDOs) to avoid duplication of standards and conflicting standards.[31] The ITU-T cooperates with the International Organization for Standardization (ISO) and the Internet Engineering Task Force (IETF).[32]

The development of recommendations are carried out by members and associates, while the executive arm of the ITU-T, the TSB, coordinates workshops and seminars in information and communications technologies. The technical work is managed by 13-study groups (SGs) and experts in telecommunications. SGs are then supported by Focus groups (FGs) to expedite the standardization needs. FGs have greater freedom to organize and finance than SGs, and involve nonmembers. Recent work includes Next Generation Networking, Internet Protocol, and digital identity management (ITU Telecommunication Standardization Sector (ITU-T)—Focus Groups).

The rise of the personal computer and rapid technology development forced the committee to streamline its approval process. The approval of a recommendation is a fast-track procedure termed the *Alternative Approval Process* (AAP). AAP was implemented in 2001. The process reduced the time of the standardization by 80–90 percent. Prior to 2001, a proposal could take four to five years for approval, but today, an initial proposal of a draft document by a member entity to final approval of a full-status "recommendation" may be accomplished in a few months. The use of electronic documents once the approval process is initiated eliminated additional physical meetings. The draft recommendation is submitted for review and, if agreed, is given consent for a final review process. TSB announces the start of the AAP process by calling for comments on the ITU-T website. The "last call" is a four-week process in which member states and sector members can submit comments. If there are no comments, but editorial corrections, the recommendation is approved. If there are comments, the SG and TSB set up a comment resolution process with the revised text posted on the web for an additional three week review process. Again, If there are no comments, but editorial corrections, the recommendation is approved. If comments are posted, the draft text and comments proceed to the next SG for more discussion and a new approval process.[33]

The ITU-T issues recommendations that have series names such as X.500. X is the series and 500 is the identifying number. The X series is described as data networks, open system communications, and security.

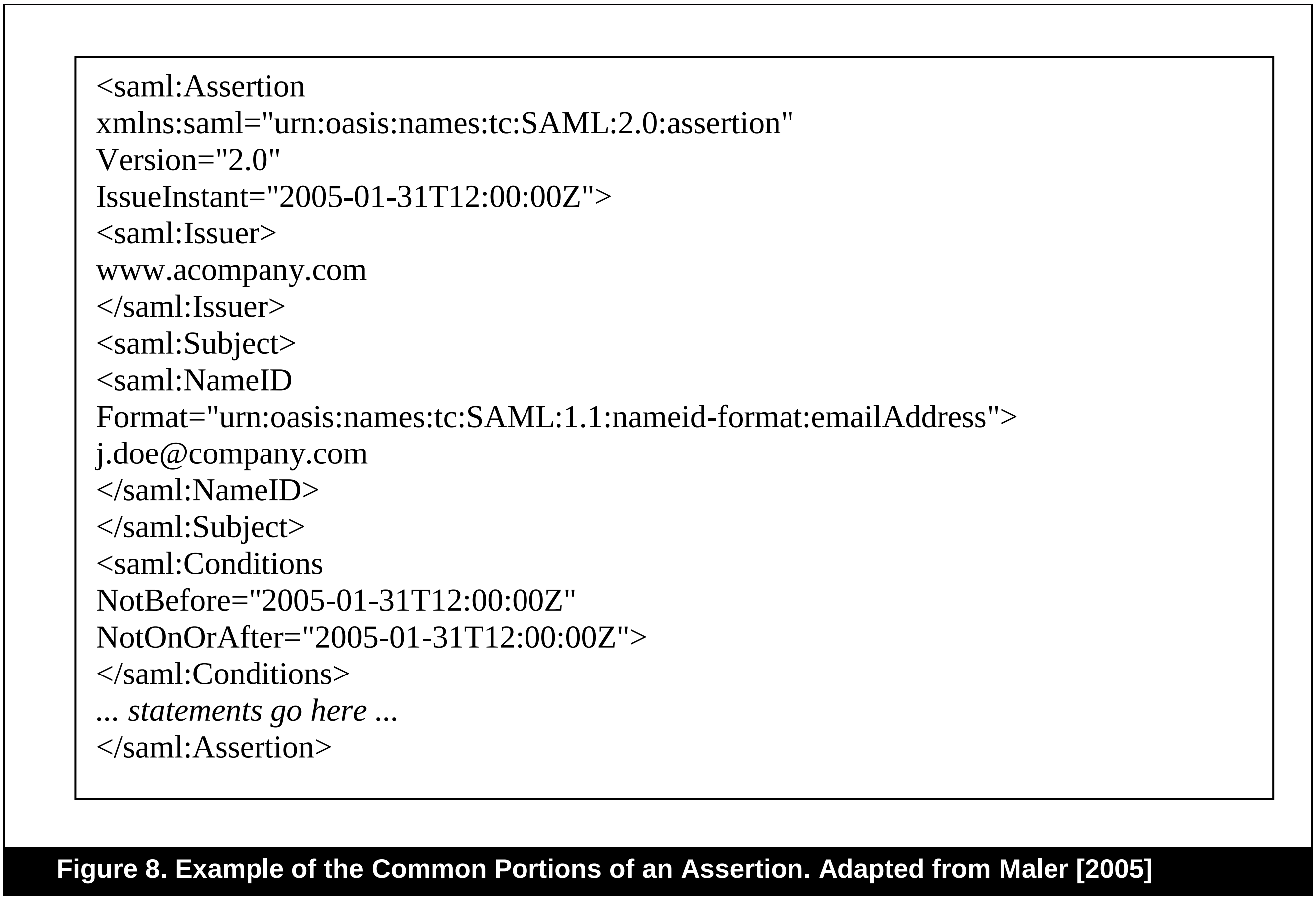
X. COMMON STANDARDS

This section describes the most common IdMS related standards. We start with Kerberos as the oldest standard still in use (most Secure Socket Layer implementations use Kerberos). The rest of the standards are organized chronologically and by the originating organization.

Kerberos[34]

Kerberos is one of the earlier security standards developed.[35] Kerberos, developed by MIT (Massachusetts Institute of Technology), is a computer network procedure that allows businesses to communicate securely over a non-secure network by proving their identity. A client-server model is used to prove mutual authentication of user and server's identities using a symmetric key cryptography and a trusted third party, rather than public key encryption. MIT developed Kerberos with some of their major vendors and users such as Sun Microsystems, Apple, Google, Microsoft, and Centrify Corporation. Kerberos version (v.) 4 was published in the 1980s. V. 5 was published in 1993 to reduce limitations and security issues of v. 4. Kerberos allows an authenticated user to log on and access all network resources required. Messages are protected against eavesdropping and replay attacks. An et al. [2006, p.176), argue that Kerobos could be a useful tool for the development of secure RFID applications. The use of RFID technology in ubiquitous applications (e.g., u-city, u-farms) is an example of a peer-to-peer (p-2-p) nomadic network.

[31] http://www.itu.int/ITU-T/50/docs/ITU-T_50.pdf (last accessed 08/16/2009).
[32] http://www.itu.int/dms_pub/itu-t/oth/0A/0F/T0A0F0000090001PDFE.pdf (last accessed 08/16/2009).
[33] http://www.itu.int/dms_pub/itu-t/oth/0A/0F/T0A0F0000090001PDFE.pdf and http://www.itu.int/ITU-T/e-flash/022-jan06.html (last accessed 08/16/2009).
[34] http://en.wikipedia.org/wiki/Kerberos_(protocol) (last accessed 08/16/2009).
[35] Versions 1 through 3 were used only internally by MIT, version 4 was published in the late 80s. Version 5 was the first to be adopted as a standard. Its first specifications were published in 1993.



```
<saml:Assertion
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Version="2.0"
IssueInstant="2005-01-31T12:00:00Z">
<saml:Issuer>
www.acompany.com
</saml:Issuer>
<saml:Subject>
<saml:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
j.doe@company.com
</saml:NameID>
</saml:Subject>
<saml:Conditions
NotBefore="2005-01-31T12:00:00Z"
NotOnOrAfter="2005-01-31T12:00:00Z">
</saml:Conditions>
... statements go here ...
</saml:Assertion>
```

Figure 8. Example of the Common Portions of an Assertion. Adapted from Maler [2005]

OASIS based Standards

SAML[36]

The Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between an IdP and a SP. SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject to other entities, such as a partner company or another enterprise application. SAML defines a standardized mechanism for the secure communication of identity information between businesses.[37] An IdP asserts information about a subject and guarantees that a user has been authenticated with certain attributes. The SP relies on the information given by the IdP [Goodrich et al. 2008; Cantor et al. 2009]. For example, Google is using SAML as a SP and can authenticate users that are trying to access secured content through "home built" IdP [Sturdevant 2007]. SAML also supports a Single Sign-On (SSO), which provides the user with the ability to authenticate in one domain while using resources in other domains without re-authenticating [Pfitzman and Waidner 2002]. Figure 8 depicts an example of assertion using SAML 2.0. Although SAML is an OASIS standard, the identity federation architecture of Liberty Alliance is compliant with the SAML 2.0 standard (Liberty Alliance Project).

SPML[38]

Service provisioning is the preparation of IT systems' resources that are required to carry out a specific action (Section IX). Provisioning automates the management of user or system's entitlements relative to electronically published services. Service Provisioning Markup Language (SPML) is an XML-based open standard that facilitates the exchange of user, resource, and service specifications information between organizations. It is used for the integration and interoperation of service provisioning requests. Figure 9 illustrates a provisioning process using SPML version 1. SPML was developed by OASIS and evolved from three earlier competing specifications [Sodhi 2004]. SPML 1.0 was accepted in 2003, and 2.0 was accepted in 2006.

[36] http://en.wikipedia.org/wiki/SAML (last accessed 08/16/2009).
[37] http://saml.xml.org/about-saml (last accessed 08/16/2009)..
[38] http://en.wikipedia.org/wiki/SPML (last accessed 08/16/2009).

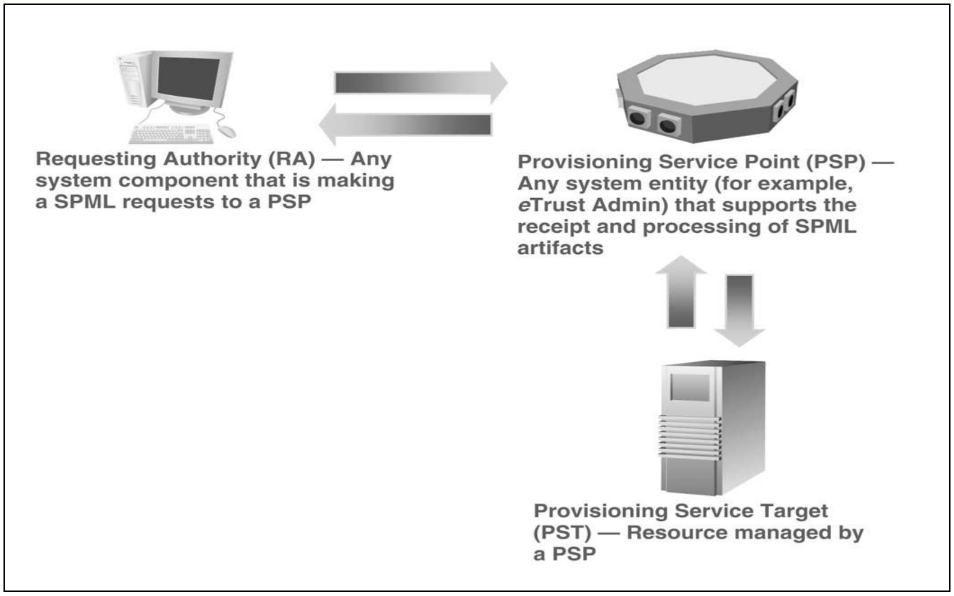

Requesting Authority (RA) — Any system component that is making a SPML requests to a PSP
Provisioning Service Point (PSP) — Any system entity (for example, *e*Trust Admin) that supports the receipt and processing of SPML artifacts
Provisioning Service Target (PST) — Resource managed by a PSP

Figure 9. Sample Business Scenario—Externalization of Provisioning Activities Using SPML. Adapted from Sodhi [2004]

Figure 9 illustrates the process used for provisioning using SPML. The requesting authority sends a request to the provisioning service (e.g., eTrust) that supports SPML. The PSP allocates resources and send a reply to the RA. As illustrated in Figure 10, a PSP might draw on resources managed by several provisioning Service Targets (PSTs) and might communicate with other provisioning services to request additional resources.

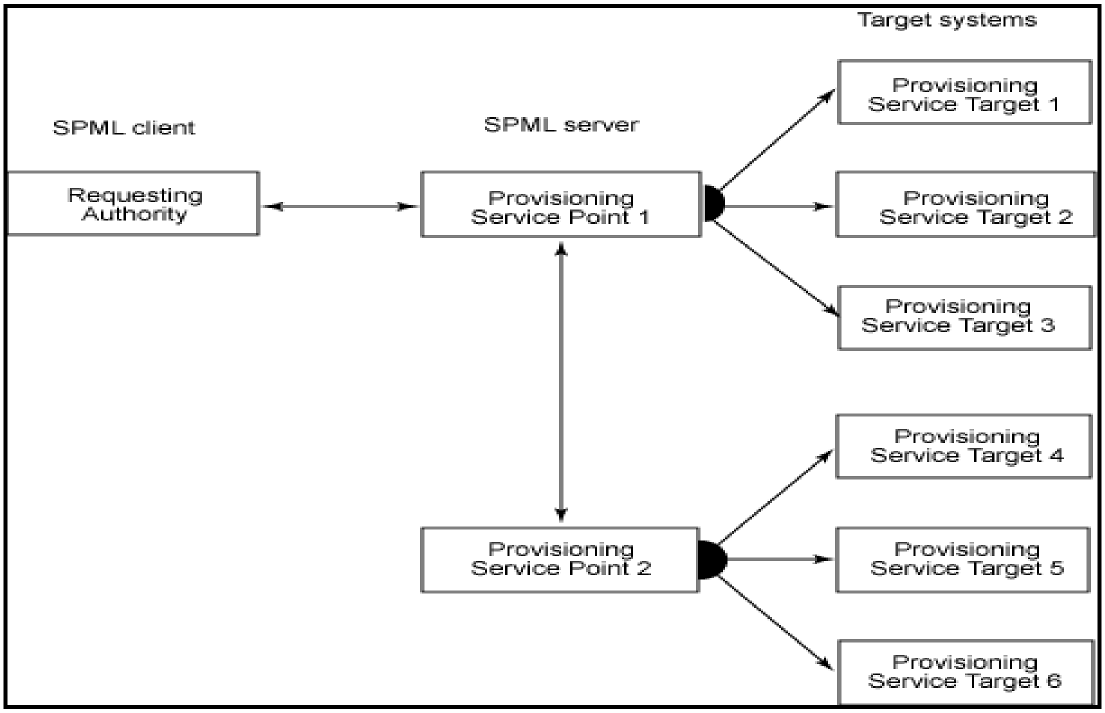

Target systems
SPML client
SPML server
Requesting Authority
Provisioning Service Point 1
Provisioning Service Point 2
Provisioning Service Target 1
Provisioning Service Target 2
Provisioning Service Target 3
Provisioning Service Target 4
Provisioning Service Target 5
Provisioning Service Target 6

Figure 10. SPML Provisioning Architecture. Adapted from Verma [2005]

SPML allows organizations to set up interfaces for web services and applications though web portals, application servers, and service centers that generate provisioning requests within and between organizations. The automation of user or system entitlement using SPML eliminates proprietary issues (e.g., silo, proprietary access solutions). Also, establishing interoperability between provisioned systems allows an organization to centrally create end-user accounts for web services and applications [Peterson 2003].

XACML[39]

The Extensible Access Control Markup Language (XACML) is a standard to describe and interpret access control policies, implemented in XML, and used as a processing model. XACML was initially developed by a consortium of companies (Entrust Inc., IBM, OpenNetworks.org, Quadrasis Inc., Sterling Commerce Inc., Sun Microsystems, and BEA Systems Inc.). Subsequently, OASIS adopted XACML as one of its standards. The first actual implementation of XACML was developed by Sun Microsystems Inc. in Java and is available at http://sunxacml.sourceforge.net. The most recent v. 2.0 was approved on February 1, 2005, and the newest v. 3.0 has been in preparation since 2007. XACML uses two main engines: Policy Decision Point (PDP) and Policy Enforcement Point (PEP). PDP evaluates the policies based on Requests. PEP is the application-specific element that enforces access to a resource, and generates requests on a PDP. Figure 11 shows an example of a request command using XACML. The example shows a user requesting access to a web site.

XACML attribues allow [Ardagna et al. 2004, p. 45]:

- The unification of access control languages; encourages reusability
- The unification of multi-application tools for managing and writing access control policies
- Extensions to the access control language to accommodate other access control policies
- One policy to contain or refer to another

```
<schema majorVersion="1" minorVersion="0">
<providerIdentifier providerIDType="urn:oasis:names:tc:SPML:1:0#URN">
<providerID>urn:oasis:names:tc:SecF</providerID>
</providerIdentifier>
<schemaIdentifier schemaIDType="urn:oasis:names:tc:SPML:1:0#GenericString">
<schemaID>PersonSchema</schemaID>
</schemaIdentifier>
<attributeDefinition name="FullName"
description="Full name of the employee joining."/>
<attributeDefinition name="email" description="E-mail address."/>
<attributeDefinition name="description" description="Description."/>
<attributeDefinition name="project" description="Project assigned to."/>
<objectclassDefinition name="employee" description="Sample employee.">
<memberAttributes>
<attributeDefinitionReference name="FullName" required="true"/>
<attributeDefinitionReference name="email" required="true"/>
<attributeDefinitionReference name="description"/>
<attributeDefinitionReference name="project" required="true"/>
</memberAttributes>
</objectclassDefinition>
</schema>
```

Figure 11. User's Request Using XACML Adapted from Ardagna [2004]

XACML's advantages over other access-control policy languages include [Russell 2003]:

- Security administrators can describe an access-control policy once, without having to rewrite it numerous times in different application-specific languages.
- Application developers do not have to invent their own policy languages and write code to support them; they can reuse existing, standardized code.

[39] http://en.wikipedia.org/wiki/XACML (last accessed 08/16/2009).

- XACML is intended to be primarily a machine-generated language. XACML creators expect that user-friendly tools for writing and managing XACML policies will be developed, since they can be used with many applications.

- XACML can accommodate most access-control policy needs and support new requirements as they emerge.

- A single XACML policy can be applied to many resources, which reduce inconsistencies and eliminate duplication of effort in creating policies for different resources.

- With XACML, one policy can refer to another. In a large organization, a policy for a specific site might reference both a companywide policy and a country-specific policy.

Liberty Alliance Project Standards

The following set of standards was developed by the Liberty Alliance project and is often discussed under the umbrella of the Identity federation framework (ID-FF). The goal of the framework is to eliminate the present "silo" approach to identity management (Section IV) and create a globally networked user identity where all attributes, rules and policies are accessible to and from each entity involved, using the concept of "circles of trust."

ID-FF[40]

ID-FF is an open-source-based framework, for creating standardized, multivendor, cross-organizational federations of identities. The term *federation* denotes a circle of organizations whose business relations are based on Liberty Alliance architecture and operational agreements where a user can perform online transactions in a seamless environment. The user is said to federate otherwise isolated account.[41]

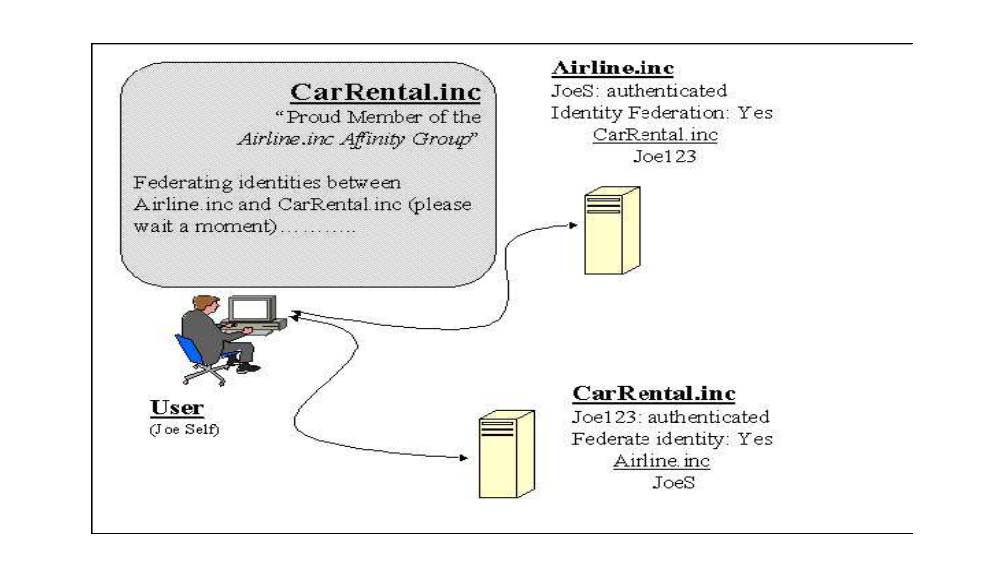


Figure 12. Federation of Local Identities. Adapted from Liberty ID-FF

As illustrated in Figure 12, ID-FF provides for two types of user experience: identity federation and single sign on (SSO). SSO builds on identity federation and provides a relatively easy to use interface. Based on the ID-FF framework, the user logs into a website (an airline in this example) and is asked if they want to federate their airline identity with any other identity that they may have in the airline's circle. Upon consent, the identities are federated.

SSO is a simplification of the federation concept. A common example is the use of portal websites such as Travelocity.com (Section VII). Once the user is logged into the portal and is authenticated, the user is considered a trusted entity. In each subsequent transaction, the user is authenticated and her attributes are available to the service provider. This approach eliminates some of the issues discussed earlier in the tutorial such as password overload. ID-FF also provides for a de-federation function, that is, the termination of a federation. ID-FF uses HTML, SOAP, and JavaScript to exchange messages between SP and IdP.

[40] http://www.projectliberty.org/liberty/resource_center/specifications (last accessed 08/16/2009).
[41] http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications.

ID-WSF[42]

In addition to ID-FF, the Liberty Alliance project defines the Identity Web Services Framework (ID-WSF) and Identity Services Interface Specifications (ID-SIS). ID-WSF v. 2.0 was announced in October 2006[43] and was built on ID-FF to support the secure and seamless development and use of web services and Service Oriented Architecture (SOA). An additional function, Liberty People Service (LPS), provides user-centric web services protocol and was developed to support users' access to web-based social networks (i.e., Web 2.0).

The standard includes the following functions: authentication of web service consumers (WSC), message protection, privacy protection, service discovery, and user interaction to obtain consents. ID-WSF was designed to work with SAML 2.0. The specification extends the concept of an IdP to define a Trusted Module (TM), which is a software module allocated to a device and is trusted. ID-WSF allows two modes: federated transactions, which establish identity relationships with the service or web service provider, and SSO transactions. An SSO may be self-asserted where the TM acts as its own IdP; facilitated where the TM facilitates the authentication of the user via a proxy (rarely used since it does not use the full capabilities of the TM), or delegated where the IdP assigns some of the single sign-on process to the TM.

ID-SIS

ID-SIS specifications are used to define an identity-based web service that maintains, and provides identity data regarding a user (i.e., user's profile). Returning to the Travelocity example, a profile would be a user's name, address, travel preferences, alerts' request, and preferred payment information. ID-SIS Employee specifications are used to define similar functionality in the workplace. An example would be an employee's directory entry with phone extension, office number, and mailbox number.

An extension of ID-SIS is the Geolocation Service (ID-SIS-GL), which provides the geolocation of a principal (a person or an object) while in motion. Some of the data provided are the geographic coordinates, direction of travel, and speed. Such services can be used to locate and/or follow an entity. The ID-SIS specifications include extensions, which enable developers (or specific implementation) to add attributes that are not defined in the original specifications. These extensions provide flexibility for various implementations.

The Liberty Alliance framework assumes the existence of a network of distributed servers that maintain users' attributes and policies. This framework might not work well for mobile, ad-hoc, and peer-to-peer architectures. In addition, users cannot federate identities that are not in the "circle." The concept of "circle of trust" also assumes that all participants are trustworthy. The latter could pose a problem if some organizations operate under different laws or regulatory frameworks (see further discussion in Section VIII).

WS-* Specifications[44]

WS-* denotes an identity management framework based on web services architecture.[45] The standard enables secure communication between organizational systems using basic web-services messaging. Web services are the current de facto standard for business-to-business communications. The WS-* framework enables developers of web services to federate identities, thus authenticate service requests across domains (and organizational systems) regardless of the policies of each domain or their format.

The **Web Services Federation** (WS-Federation) is a mechanism that allows divergent businesses to share user and computer systems securely through identity authentication and authorization. WS-federation policies provide a basic trust model between identity providers and dependent parties through WS-Security, WS-Trust, and WS-Security Policy. The standard is based on the concept of a token but does not restrict users to a given token structure or format. WS-Federation allows access from web clients using HTTP or from web-services clients directly. Claims (or assertions) about the entity requesting the service (the requestor) are codified into a token. WS-Trust is the component that defines the Security Token Service (STS) and the protocol used to request or issue the token. WS-SecurityPolicy describes the STS and its associated claims.

[42] http://iiw.idcommons.net/Liberty_Alliance_ID-WSF (last accessed 08/16/2009).
[43] http://xml.coverpages.org/LibertyID-WSFv20.html (last accessed 08/16/2009).
[44] http://www.ibm.com/developerworks/library/specification/ws-fed/ (last accessed 08/16/2009).
[45] http://xml.coverpages.org/WS-FederationDemo.html (last accessed 08/16/2009).

```
<s:Envelope>
  <s:Header>
    <wsa:Action>
      http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue
    </wsa:Action>
    <!-- Other headers not shown for brevity -->
  </s:Header>
  <s:Body>
    <wst:RequestSecurityToken>
      <wst:TokenType>
        http://example.org/mySpecialToken
      </wst:TokenType>
      <wst:RequestType>
        http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
      </wst:RequestType>
    </wst:RequestSecurityToken>
  </s:Body>
</s:Envelope>
```

Figure 13. Example Request Security Token (RST) message[46]

WS-Security is a communications protocol enabling the application of security to web services. The standard provides the integration of security aspects by permitting and brokering trust of identities, attributes, and authentication of web services users. **WS-SecurityPolicy** is a specification that allows web services to use XML to describe and advertise their policies and for web service consumers to specify their policy requirements. It is a W3C recommendation. **WS-Trust** is the protocol used for requesting, issuing, renewing, canceling, and validating security tokens.[47] Each entity has its own policies which define their STS and associated claims. WS-Trust is implemented in web services (proprietary or open source) provided by companies such as Microsoft and Sun Microsystems. The process begins by the requestor identifying a service it would like to access. Subsequently, the requestor inquires as to the level of security needed to access the service (using WS-SecurityPolicy). If the requestor does not have the appropriate level of security, it can request one from the STS. The STS issues an identity token and associated claims for the requestor (based on eligibility). The relying party[48] (or SP) accesses the STS to validate the requestor's token and claims. Figure 13 provides sample code illustrating a token request message.

WS-Federation and its subcomponents were jointly developed by a consortium of companies (i.e., BEA Systems, BMC Software, CA Inc., IBM, Layer 7 Technologies, Microsoft, Novell, and VeriSign). WS-security was initially developed by IBM, Microsoft, and VeriSign and was adopted by OASIS in 2007. One of the advantages of WS-Federation is that it can be used directly by Simple Object Access Protocol (SOAP) clients and web services. WS-Trust protocol and WS-Federation extensions are expressed in a browser-based location (client based). This provides federated identity operations a universal model for web services and browser-based applications. Unlike server-based standards, browser-based are portable and can be implemented on mobile devices and in peer-to-peer applications where the concept of a stable server does not exist.

ITU-T Standards

X. 509[49]

X.509 is an ITU Telecommunication Standardization Sector (ITU-T) standard developed based on the concept of Public Key Infrastructure (PKI). X.509 certificates are supported by most current security protocols such as Secure Socket Layer/Transport Layer Security (SSL/TLS), IPSec (Internet Protocol security), and Secure Multipurpose Internet Mail Extensions (S/MIME). A trusted third party, the certification authority (CA) issues a certificate to be

[46] http://msdn.microsoft.com/en-us/library/bb498017.aspx (last accessed 08/16/2009).
[47] http://en.wikipedia.org/wiki/WS-Trust (last accessed 08/16/2009).
[48] The term relying party, relying entity or relying service is often used to describe the service provider (SP), since these entities rely on the authentication process.

used by a particular business (or entity). The certificate is unique to the business and thus can authenticate any message it sends.

X.509 maintains certificates in a "tree like" structure. The attributes (or the level of trustworthiness) of the root certificate are inherent in subsequent (son) certificates. Authenticity and authority of the certificate are dependent on the origin or "root" certificate, which is trusted.[50] An example of a "root" certificate is a certificate used by a web browser to verify users' identity within SSL or TSL secure connections. The certificate must pass through the certification revocation list (CRL). A CRL is a list of serial numbers of certificates that have been rejected or are no longer in use.[51] This enables the automatic revocation of rights.

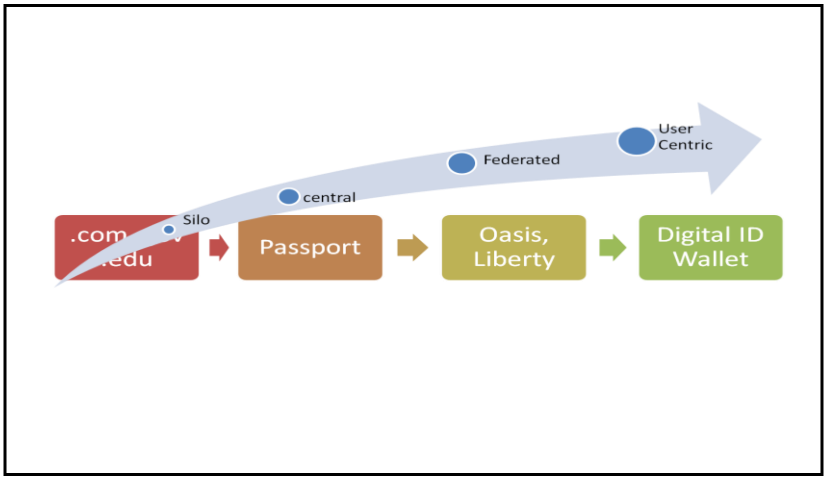


Figure 14. From Silo to User Centric Approach to Identity Management. Adapted from Cho [2006]

Digital ID wallet[52]

Digital ID wallet is an ITU-T international standard (Self-Control Strengthening-Type Digital Identity Sharing Framework) developed initially by the Electronics and Telecommunications Research Institute (ETRI) in South Korea. The digital ID wallet is essentially a web-based cyber wallet that serves as storage for data such as addresses, telephone numbers, user's ID, and passwords. The underlying philosophy of the standard is to move beyond the concept of federated identity and develop user-centric IdMS.

Figure 14 illustrates the conceptual progression from the initial silo approach through centralized (e.g., Microsoft's Passport), and federated to user-centric.

One of the challenges with federated identities is the need for interoperability between various providers who often have differing policies and architecture. The larger the number of providers involved, the more complex the federation. Although consortia like Liberty and OASIS membership span a variety of industries and countries, they are not universal. Using federated identities, users are forced to use member websites or services (or websites that are part of the "circle of trust"), reducing flexibility especially for users in less compliant countries. Furthermore, federated identities shift the control from the user to the service and identity providers. The Digital ID wallet standard attempts to address these challenges. A key attribute of the ID wallet is that the key is generated using the user's id and not a Certification Authority. This approach is independent of the existence of a Certification Authority and is well-suited to support mobile and ad hoc communication.

The system automatically creates a secure secret key for each web site, which is stored in a client-based digital wallet. Thus, it is not necessary for users to memorize individual passwords. The Digital ID wallet enables the user to register and log onto a website, store personal information, and other data at any time. Users can use the Digital ID wallet to pay for online purchases. The Digital ID wallet is based on mutual authentication technology, which

[49] http://www.tech-faq.com/x.509.shtml (last accessed 08/16/2009).
[51] http://en.wikipedia.org/wiki/Certificate_revocation_list (last accessed 08/16/2009).
[52] http://english.hellodd.com/jinny_board/board/chk_content.asp?table=newpro_board&idx=8 (last accessed 08/16/2009).

protects users' information from phishing and farming attacks. Jung et al. [2007] proposed a framework for the implementation of a mobile Digital Id wallet. The key challenge in the development of a mobile ID wallet is that user information resides in a Universal Subscribers Identity Module (USIM) and not with a Service Provider. M-commerce is highly developed in Asian countries such as Japan and Korea and thus requires advanced security features. In addition, "the mobile Digital ID wallet provides related services that perform sharing and managing of personal and certification information" [Jung et al. 2007, p. 1].

The main advantage of the standard is that it is client-based and can be applied to a variety of websites, policies, and architectures. The biggest challenge for the implementation of the Digital ID wallet is its dependence on the casual end-user. Users should be aware of the possibilities and obstacles of the standard and versed in proper definitions and use of the digital wallet.

XI. VENDOR IMPLEMENTATIONS

The IdMS Market

According to IDC, the market of IdMS technology is likely to increase to $5.1 billion by 2010 [Kho 2009]. A Forrester report estimates the market will reach $12.3 billion by the year 2014 [Cser and Penn 2008]. These figures include revenues from software and implementation services [Cser and Penn 2008]. Overall, the security vendors' market is expanding rather than converging (as often is expected from a maturing market). Based on Forrester, 17 percent of the new vendors' offerings announced in 2007 were related to Identity and Access management. Within the IdMS market, provisioning licensing and services account for 50 percent of the revenue and is expected to grow by approximately 25 percent. By 2014, provisioning is expected to account for 64 percent of the IdMS market. SSO (enterprise and web) are expected to grow by 28.5 percent and 6.9 percent respectively. Sixty-seven percent of implementations are in North America, 26 percent in Europe and 6 percent in Asia Pacific. Cost and complexity are publicized as the main reasons companies delay the implementation of IdMS solutions.

As of Feburary 2008, Forrester listed approximately thirty companies, specializing in eight services, from enterprise SSO (e-SSO) to provisioning, entitlement management, and identity audits [Cser and Penn 2008]. The number of vendors that offer a suite of solutions is relatively small, and the solutions are partial at best. Cser and Penn's [2008] study also analyzed eleven leading IdMS vendors to find that none offers all the potential services. Out of the eight services listed, IBM, Novell, and Oracle are leading with six full services and one partial, followed by Sun with six services and Computer Associates with five full services and two partial. The remaining vendors offer anywhere from three to four services.

This market fragmentation and specialization is slowing down adoption. Presently, companies are forced to implement fragmented solutions from a variety of vendors, increasing complexity and cost. For example, all eleven major vendors offer provisioning services, while only three of the vendors offer virtual directories. In June 2008, Forrester published an analysis of fourteen IdMS related technologies [Cser 2008]. Estimated implementation costs of these services vary widely, from $30,000–$50,000 for services such as password management to $500,000–$630,000 for services such as provisioning and role management.

Vendors' Offerings

Overall, the market of IdMS includes some integrated solutions from large IT companies such as IBM, Oracle, Sun, and Microsoft. For example, Microsoft is attempting to secure "cloud" services using WS-based identity management solutions within its web-services offerings. In addition, the market includes IT security "mega-vendors" such as Checkpoint Software, McAfee, and Symantec, and a large number of small companies offering one or more specialized, innovative services. Although the frameworks and standards discussed in this tutorial are slowly attempting to converge around an open source, federated, XML based approach to IdM, the technologies and services available to companies are highly fragmented, leading to costly and complex implementations.

IBM[53]

IBM markets its solution under the Tivoli® Identity Manager (ITIM) trademark. IBM's website claims that ITIM is a tool, which enables automated, policy-based user management. The package supports an e-SSO and a Web SSO, strong authentication capabilities, role-based, group or request-based provisioning, and most open standards and specifications such as SAML, Liberty Alliance ID-FF, and WS-Security specifications such as WS-*[54]. Tivoli includes the following features [IBM 2007]:

[53] http://www-01.ibm.com/software/tivoli/ (last accessed 08/16/2009).

[54] http://www.nasi.com/tivoli_identity-management.php (last accessed 08/16/2009).

1. Automated user management throughout the entire user's life cycle.
2. Policy driven IdM, audit trails and reports to support organizational compliance with regulations such as SOX. Any change to the system that does not comply with organizational or regulatory policies cannot be implemented.
3. Web-based user support to reduce reliance on helpdesk.
4. Support of millions of users with relatively little performance or availability concerns.
5. A large set of functions for "out-of-the-box" use and customization capabilities. These functions are J2EE based and support IBM and Microsoft environments.
6. Simulation capabilities that enable the organization to evaluate a policy change and its potential unintended consequences prior to implementation.

ITIM mostly supports IBM or Microsoft architecture, limiting its implementation to organizations that use one of these two architectures. For example, transactions are stored in only one of three common proprietary databases (i.e., Oracle, DB2, or SQL Server). ITIM supports users and services as entities.

SUN Microsystems[55]

Sun Microsystems (Sun) markets their identity management software under the trademark Identity Manager 8.0 (SIM). The product supports role based provisioning and life cycle management. SIM provides audit trails, and enables the export of generated data to other repositories for further analysis and reporting. Similar to ITIM, SIM is policy driven and is geared to enhance compliance with external regulations. SIM reports 99.9 percent uptime and scalability of up to millions of users with limited reduction in performance.[56] SIM is compatible with SPML 2.0 and operates in more environments than ITIM (e.g., Sun Solaris, Red Hat Linux, HP OpenVMS, HP-UX, IBM AIX, IBM OS/400, Microsoft Windows, SuSE Enterprise Linux) and supports a larger number of databases and enterprise applications than ITIM.

Novell[57]

Novell identity manager (IDM) is part of a suite of access and security control products offered by Novell Inc. It includes similar features to the ITIM by IBM and the SIM by Sun. However, it supports a larger variety of architectures (e.g., operating systems, database, enterprise software, and messaging) than the other two packages. Most systems are supported "out-of-the-box" while some need customization. IDM is XML based and offers user-friendly interface, self-management, testing, and policy based management. Although Novell IDM was one of eight vendors approved by Liberty Alliance as SAML compliant, it was not possible to find compliance or standard related information on Novell's website. While Sun emphasis its compliance with a large number of open source standards, Novell does not.

Shibboleth[58]

Shibboleth is a semi-commercial endeavor developed in the United Kingdom by the Joint Information Systems Committee (JISC) to support federated identity management across all educational institutions. Shibboleth is a SAML based product and was developed for use over Internet II. Access control is based on a set of attributes provided by an IdP and a set of rules defined by an SP. If a user's attributes match the SP's rules, the user is granted access. The basic premise is the existence of a countrywide (currently implemented in the U.K.) "circle of trust" where institutions trust the information provided by others in the circle. The goal of the project is to have anyone (students, professor, administrators, and researchers) involved in UK's educational system (elementary school to higher education) enrolled in Shibboleth, to facilitate ease of access to educational resources and resource sharing. Additional information can be found at http://en.wikipedia.org/wiki/Shibboleth (Internet2) and at http://www.jisc.ac.uk/whatwedo/themes/accessmanagement/federation/animation.

[55] http://www.sun.com/software/products/identity_mgr/index.xml (last accessed 08/16/2009).
[56] http://www.sun.com/software/products/identity_mgr/features.xml (last accessed 08/16/2009).
[57] http://www.novell.com/rc/docrepository/public/16/basedocument.2007-03-13.3695433449/4641008_en.pdf (last accessed 08/16/2009).
[58] http://en.wikipedia.org/wiki/Shibboleth.

XII. CONCLUSIONS

We began the tutorial by describing several conceptual frameworks for the implementation of IdM systems and concluded by detailing current standards and vendors' implementations. The tutorial also introduced social and technical challenges that need to be resolved.

Although we are seeing some progress in the development of universally accepted frameworks and technologies for the management of cyber identities, much work remains. The various paradigms and implementations need to converge. At present, we are seeing two different approaches to IdMS. One is based on a circle of trust, which enables transparent IdMS for users within the circle. This approach creates islands that are not interoperable, limit accessibility outside of the circle, and possibly leading to an increase divide between organizations in compliant countries and nonparticipating countries. This federated approach relies on trusted and managed identity and service providers. These providers could become an attractive target for hackers.

The user-centric approach enables users to access any website at any time and any place. However, it depends on users' ability to manage their identities, policies, and privacy, a task that requires awareness and training. Designers of user-centric systems need to create user-friendly interfaces and a transparent environment. Resolving these issues also depends on the development of globally accepted policies. Much like our presently universal telephone system, which heavily depends on a universal infrastructure, cost structure, and operational policies, a universal implementation of an IdMS requires global acceptance.

As we move on to a society based on the "Internet of things" or ambient intelligence, security will become more complex. Identities will extend beyond people, organizations, and services to everything. For example, it is possible that as you leave the house in the morning, your smart shoe will send a service request to weather.com, which in turn will ask for a geolocation from your shoe. If weather.com predicts a warm day, air vents will open to create airflow to your shoe. Similar scenarios might exist with your smart clothing, home, and car. It is up to each individual user to determine how much information each of these items is allowed to send, how often, when, and to which service. Such scenarios could result in privacy issues that need to be resolved such as how long the requested information is to remain with the service provider and what the provider can use it for.

Finally, globalization depends on our ability to develop a universal IdMS. However, jurisdictional issues, legal and cultural differences might slow the progress of such endeavors. Although these are pertinent and interesting topics, they are beyond the scope of this tutorial.

ACKNOWLEDGMENTS

This tutorial was originally presented at the Americas Conference on Information Systems, San Francisco, CA, August 2009.

We would like to thank Dr. Jean-Henry Morin and Dr. Paul Gray for their insightful suggestions and comments.

The following items have been reproduced with permission of the copyright holder and require citation of the source if reproduced further.

- Figures 6 and 7: Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
- Figure 8: This presentation may be copied and reused with attribution. Eve Maler (eve.maler@sun.com).
- Figures 9 and 11: Copyright clearance from Elsevier (10/22/2009).
- Figure 13: (c) 2007 International Business Machines Corporation, and Microsoft Corporation, Inc.. All rights reserved. IBM and Microsoft (collectively the "Authors") hereby grant permission to copy and display the "Understanding WS-Federation" paper (the "Document"), in any medium without fee or royalty, provided that you include the following on ALL copies of the Document, that you make.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to world wide web pages. Readers who have the ability to access the web directly from their word processor or are reading the paper on the web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Alrodhan, W.A., and C.J. Mitchell (2008). "A Client-side CardSpace-Liberty Integration Architecture," Presented at IDtrust, Gaithersburg, MD., 4–6 March, pp. 1–7, Copyright 2008 ACM978-1-60558-066-1.

An, K., K. Lee, and M. Chung Design (2006). "Design and Implementation of an RFID-based Enterprise Application Framework based on Abstract BP and Kerberos," *International Journal of Information Processing Systems*, (2)3, pp. 170–177.

Ardagna, C.A., et al. (2004). "XML-based Access Control Languages," *Information Security Technical Report* (9)3, p. 45.

Cameron, K. (2005). "The Laws of Identity," http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (current 23 July 2009).

Cameron, K., and M.B. Jones (2006). "Design Rationale behind the Identity Metasystem Architecture," p. 1–11, *Microsoft Corporation*, http://www.identityblog.com/wp-content/resources/design_rationale.pdf (current 23 July 2009).

Cantor, S., et al. (eds.) (2005). "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML), http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf (current 23 July 2009).

Cazier, J.A., and C.M. Botelho (2007). "Social Engineering's Threat to Public Privacy," Proceedings of the 6th Annual Conference on Information Security, Las Vegas, Nevada, 11–12 April.

Cervesato, I., et al. (2008). "Breaking and Fixing Public-key Kerberos," *Information and Computation* (206), pp. 402–424.

Cho, S. (2006). "Present and Future Trend of Digital Identity in Korea", Presented at the ITU-T Workshop on "Digital Identity for NGN." Geneva, 5 December, http://www.itu.int/ITU-T/worksem/ngn/200612/abstracts.html (current 22 July 2009).

Coffee, P. (2003). "Port Scans- Security's Language," *News & Analysis, eweek*, 23 April, p. 34.

Cser, A. (2008). "Forrester TechRadar™: Identity and Access Management," Forrester Research, Inc., 18 June, pp. 1–24.

Cser, A., and J. Penn (2008). "Identity Management Market Forecast: 2007 to 2014," Forrester Research, Inc., 6 February, pp. 1–16.

Dimiani, D., D.S. Capitani di Vimercati, and P. Samrati (2003) "Managing Multiple and Dependable Identities," In the proceeding of the *IEEE Internet Computing*, Published by the IEEE Computer Society, November/December.

Goodrich, M.T., R. Tamassia, and D. Yao (2008). "Notarized Federated ID Management and Authentication," *Journal of Computer Security* (16), pp. 399–418.

IBM (2007). "Succeeding with Automated Identity Management Implementations," White paper, IBM Corporation, March, pp. 1–12, http://www-01.ibm.com/software/dk/tivoli/security/pdf/Identity_Management_Implementations.pdf (current 23 July 2009).

Jung, Y.S., et al. (2007). "A Secure Mobile Digital ID Wallet using USIM of 3GPP," Supported by IT R&D program of MIC/IITA, 2007 Research Fund of Kookmin University & Kookmin Research Center UICRC (Korea), and MIC (Ministry of Information and Communication), http://recerca.ac.upc.edu/eurongi08/ext-abs/5-2.pdf (current 23 July 2009).

Kellomak, S. (ed.) (2003). "Liberty ID-SIS Employee Profile Service Specification," Version 1.1, Liberty Alliance Project, pp. 1–20, http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_sis_1_0_specifications (current 21 July 2009).

Kho, N.D. (2009). “The Changing Face of Identity Management,” *EContent*, April, pp. 21–25, http://www.econtentmag.com/Articles/Editorial/Feature/The-Changing-Face-of-Identity-Management-53162.htm (current 21 July 2009).

Koch, M., and W. Worndl (2001). “Community Support and Identity Management,” Prinz, W., M. Jarke, Y. Rogers, K. Schmidt, and V. Wulf (eds.). Proceedings of the Seventh European Conference on Computer-Supported Cooperative Work, September 16–20, Bonn, Germany, pp 319–338, © 2001 Kluwer Academic Publishers, Printed in the Netherlands.

Maler, E. (2005). “SAML V 2.0-basics,” Sun Microsystems, http://xml.coverpages.org/Maler-SAMLV20-Basics-200610.pdf (current 21 July 2009).

Papastergiou, S., A. Karantjias, and D. Polemi (2007). “A Federated Privacy-enhancing Identity Management System,” 16th Annual IEEE Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC’07).

Peterson, T. (2003). “Quick Study: Services Provisioning Markup Language (SPML),” *Computerworld*, 00104841, 20 October (37)42, http://www.computerworld.com/s/article/86225/SPML (current 19 Oct. 2009).

Pfitzmann, A., and M. Hansen (2006). “Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management—A Consolidated Proposal for Terminology,” Version 0.28, 29 May, pp. 1–54, http://dud.inf.tu dresden.de/literatur/Anon_Terminology_v0.28.pdf (current 23 July 2009).

Pfitzmann, B., and B. Waidner (2002). ”Token-based Web Single Sign-On with Enabled Clients,” *IBM Research Report*, RZ 4358(03884), November.

Russell, K. (2003). “Quick Study: Extensible Access Control Markup Language (XACML),” *Computerworld*, 00104841, 19 May, (37)20, http://www.computerworld.com/s/article/81295/XACML (19 current October 2009).

Sidharth, N., and J. Liu (2007). “IAPF: A Framework for Enhancing Web Services Security,” In the proceedings of the IEEE 31st Annual International Computer Software and Applications Conference (COMPSAC 2007), The Computer Society.

Sliwa, C. (2003). “OASIS Ratifies Access-Control Standard,” *Computerworld*. 00104841, 24 February (37)8.

Sodhi, G. (2004). “User Provisioning with SPML," *Information Security Technical Report* (9), pp. 86–96, No. 1363–4127/04/ⓒ 2004, Elsevier Ltd.

Steiner, P. (1993). “On the Internet Nobody Knows You Are a Dog,” *New Yorker* (69)20, 5 July.

Sturdevant, C. (2007). “SAML Ups Ante of Google Apps,” *eweek*, 18 June, p. 48.

Tourzan, J., and Y. Koga (2009). “Liberty ID-WSF Web Services Framework Overview”, Version 1.1, Liberty Alliance Project, pp. 1–30, http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_1_1_specifications (current 23 July 2009).

Verma, M. (2005). “XML Security: Manage Identities More Effectively with SPML”, January 5, http://www.ibm.com/developerworks/xml/library/x-secspml1/ (current 23 July 2009).

Wason, T. (2009). “Liberty ID-FF Architecture Overview,” Version 1.2, Liberty Alliance Project, pp. 1–44, http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications (current 23 July 2009).

Whitman, M.E., and H.J. Mattord (2005). *Principles of Information Security*, Boston: Course Technology Cengage Learning.

APPENDIX A: AN EXAMPLE OF THREE APPLICATIONS AND THEIR UNIQUE DIGITAL IDENTITY NEEDS

Each of the following three domains represents some unique characteristics in the context of IdM that are interesting to explore: healthcare, e-Government, and e-learning.

Health Care

Identity management in the healthcare industry has been at the forefront of recent IdMS studies. The Health Information Privacy Act (HIPAA) was the first attempt to legislate industry specific information assets. Although HIPAA was originated in the U.S, its essence is universal as many countries adopted similar measures to protect the dissemination of medical information and patient privacy. In addition to being regulated, *Healthcare Information Systems* (HIS) are unique since:

1. A large number of stakeholders require access to a patient's information (doctors, nurses, lab technicians, billing clerks, and the patients themselves).

2. The information is created in various locations (doctor's office, a laboratory, a pharmacy).

3. The stakeholders are not co-located and, therefore, require remote access.

4. The stakeholders belong to various organizations, with various computing capabilities, security levels, and architecture, making integration difficult. Furthermore, some large medical providers (such as Kaiser Permanente) make their personal records available to individual patients from their home computers.

5. Due to the nature of their work, stakeholders (e.g., physician, specialists), require continuous and multiple access to patient records. For example, a physician might check a medical record in her office, using a desktop computer, before visiting a patient's bed. During rounds, the physician wants to re-evaluate the records and might also need to examine x-rays and lab results on a mobile device. Any IdMS should allow users the ability to toggle between applications and patients with minimum time and effort.

6. Time is of the essence. Occasionally a timely medical treatment is crucial and more important than privacy or policies. A healthcare related IdMS should take into consideration the occasional emergencies and enable exceptions.

e-Learning

Unlike Healthcare Information Systems, securing *e-learning* is voluntary and not regulated. Universities implement e-learning as a competitive advantage, a marketing tool, and to attract non-traditional students (working adults, military, foreign). For the most part, the information exchanged is not sensitive with the exception of some administrative systems (grades, transcripts and matriculation). In addition, university security requirements are lower than most other industries (mostly due to the concept of academic freedom). E-learning has the following unique characteristics (http://celsr.nova.edu/):

1. Some internal stakeholders have a stake in sharing their identities rather than following policies, whereas in most other organizations, internal users might share identities mostly by mistake.
2. Students could have someone else take a remote examination, submit an assignment, or participate in online chat for them.
3. The amount of face-to-face communication is relatively low.
4. Stakeholders are transient. Unlike other organizations, students spend only a fraction of their career at school. This is especially true with remote students who are working and have other scheduling obligations. Therefore, their level of loyalty to the organization (school) is relatively low compared with a traditional worker.
5. The goal of the university and the students conflict: The university wants to administer controlled education; degrees are conferred on successful candidates. The student wants to gain a degree. Thus, traditional identification control measures and mechanisms do not work well in e-learning environments

In short, Universities offering e-learning, unlike most traditional organizations, are defending against internal, intentional misuse by transient stakeholders with minimal organizational ties and loyalty.

e-Government

E-government systems offer a variety of services to citizens of a country (limited in reach). Most early systems were informational only and, therefore, did not pose security threats. However, over time these systems became more interactive (e.g., tax filing, automobile registration). E-government systems, if not well protected, enable hackers' access to sensitive information. E-government systems should have the following characteristics.[59]

1. Open to all citizens, yet protected from "unwanted entities"
2. Highly protected to prevent identity theft
3. Unauthorized access to certain systems can result in cyber terrorism.
4. In democratic societies, access control to these systems should be regulated by the legislators rather than mandated by government (executive branch).
5. Any access control implemented has to maintain user privacy.

Some of these requirements are conflicting. For example, how does one open a system to its citizens yet close it to its enemies? The Internet transcends national boundaries, and, once a system is placed in cyberspace, it is accessible to all. Similarly, the balance between a strong identity and privacy is delicate and a sensitive issue, especially when governments are involved.

APPENDIX B: COMPARISON OF THE TWO EXISTING IDMS PARADIGMS

Table B-1 compares the two main existing IdMS paradigms. The digital Identity assumes that each entity carries its credentials on the client and manages them like a key. A key provides access to certain sites based on the entity's credentials. The federated paradigm assumes a circle of trust, once an entity is allowed into the circle, it can use all the assets allocated to it.

Table B-1. Comparison of Two Paradigms

	Token	Federated
Standard	ITU-T	Liberty/OASIS
Paradigm	User centric	Circle of trust
Implementation	Client based Digital identity/key	Third party based Certificate
Advantages	User control Supports mobile and peer-to-peer communication	Third party audit ability and accountability
Challenges	• User training and awareness • More difficult to maintain the "safety" of the key • Who is authorized to issue a key? How is this entity being regulated?	• Who is "in" the circle? • Maintaining the integrity of the circle • Less effective for ad-hoc communication
Companies	Microsoft; ETRI	IBM, SUN

[59] Partially based on a report by the national science and technology council subcommittee on biometrics and identity management published in September 2008.

APPENDIX C: GLOSSARY

Action: The type of access that is being requested (for example, read, write, create, delete, logged).

Attribute: A specific characteristic of a subject, resource, action, or environment in which the access request is made. Attributes could include a user's name, workstation identity, security clearance, the file to which access is desired and the time of day.

Bag: An unordered collection of attributes, used for matching attributes to conditions. Bags may contain duplicate attributes or be empty.

Certificate authority or **certification authority** (**CA**)**:** An entity that issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes (http://en.wikipedia.org/wiki/Certification_authority).

Certification path validation algorithm: The algorithm which verifies that a given certificate path is valid under a given public key infrastructure (PKI) (http://en.wikipedia.org/wiki/Certification_path_validation_algorithm).

Directory Services: The software system that stores, organizes, and provides access to the information in a directory.

Federation: A collection of security domains that have established relationships for sharing resources in a secure manner.

Identity provider or OpenID provider: A service provider offering the service of registering, and authenticating an id.

Liveliness: Validating liveliness is part of the ID-FF framework. Its goal is to ensure that the person performing an activity at time t+1 is the same person that was authenticated and federated at time t.

Policy: A single access-control policy expressed through a set of rules.

Policy Set: A container of policies, including references to remote policies.

Provisioning: The process of preparing and equipping a network so that it can provide (new) services to its users (http://en.wikipedia.org/wiki/Service_provisioning).

Pseudonymity: Derived from pseudonym, meaning false name, and anonymity, meaning unknown or undeclared source. The pseudonym identifies a holder, that is, a human being, a service, or a machine that possesses but do not disclose their true identity.

Public key certificate (or **identity certificate**): An electronic document which uses a digital signature to bind together a public key with an identity (http://en.wikipedia.org/wiki/Public_key_certificate).

Replay attack: A form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed (http://en.wikipedia.org/wiki/Replay_attack).

Resource: A device, data element or file for which access is requested.

Revocation: The automated removal of privileges, assertions, or credentials of an entity.

Root certificate: Either an unsigned public key certificate or a self-signed certificate that identifies the Root Certificate Authority (CA). A root certificate is part of a public key infrastructure scheme (http://en.wikipedia.org/wiki/Root_certificate).

Service provider (SP): An entity that provides services to other entities. Usually this refers to a business that provides subscription or web service to other businesses or individuals (http://en.wikipedia.org/wiki/Service_Provider). SP are also referred to as relying party.

Single sign-on (**SSO**)**:** A property of access control of multiple, related, but independent software systems. With this property, a user logs in once and gains access to all systems without being prompted to log in again at each of them (http://en.wikipedia.org/wiki/Single_Sign-On).

Subject: The person, computer, or service making a request; also known as an entity or the requestor.

Target: A set of simplified conditions for the subject, resource, and action that must be met for a policy set, policy, or rule to apply to a given request.

Trusted third party (TTP): An entity which facilitates interactions between two parties who both trust the third party; they use this trust to secure their own interactions. For example, a certificate authority (CA) (http://en.wikipedia.org/wiki/Trusted_third_party).

WS-Federation: An Identity Federation specification, developed by BEA Systems, BMC Software, CA, Inc., IBM, Layer 7 Technologies, Microsoft, Novell, Ping Identity, and VeriSign (http://en.wikipedia.org/wiki/WS-Federation).

WS-Policy: A specification that allows web services to use XML to advertise their policies (on security, Quality of Service, etc.) and for web service consumers to specify their policy requirements (http://en.wikipedia.org/wiki/WS-Policy).

WS-Security (**Web Services Security**): A communications protocol providing a means for applying security to web services. On April 19 2004 the WS-Security 1.0 standard was released by Oasis-Open (http://en.wikipedia.org/wiki/WS-Security).

WS-SecurityPolicy: A web services specification, created by IBM and 12 co-authors, which deals with defining "policy assertions" which are utilized by the WS-Security, WS-Trust, and WS-SecureConversation specifications (http://en.wikipedia.org/wiki/WS-SecurityPolicy).

WS-Trust: A WS specification and OASIS standard that provides extensions to WS-Security, specifically dealing with the issuing, renewing, and validating of security tokens, as well as with ways to establish, assess the presence of, and broker trust relationships between participants in a secure message exchange (http://en.wikipedia.org/wiki/WS-Trust).

APPENDIX D: ABBREVIATIONS

AAP—Alternative Approval Process

ACL—Access Control Lists

BDT—Telecommunication Development Bureau

BR—Radiocommunication Bureau

CA—certification authority

CCIR—International Radio Consultative Committee

CCITT—International Telephone and Telegraph Consultative Committee

CPU—central processing unit

CRL—certification revocation list

CU—control unit

DNS—Domain Name System

DSML—Directory Service Markup Language

e-SSO—enterprise Single Sign-On

ETRI—Electronics and Telecommunications Research Institute

FGs—focus groups

HIPAA—Health Information Privacy Act

HIS—Healthcare Information systems

HTML—Hypertext Markup Language

HTTP—hypertext protocol

ID-FF—Identity Federation Framework

ID-SIS—Service Interface Specifications

ID-SIS-GL—Service Interface Specifications Geolocation Service

ID-WSF—Identity Web Services Framework

IDC—Interactive Data Corp

IDM—Novell identity manager

IdM—Identity Management

IdMS—Identity Management Systems

IdP—identity provider

IETF—Internet Engineering Task Force

IMS—information management systems

IOS—Inter-organizational systems

IP—internet protocol

IPSec—Internet Protocol security

ISO—International Organization for standardization

ITIM—Tivoli® Identity Manager

ITU—International Telecommunication Union

ITU-D—Telecommunication Development Sector

ITU-R—Radiocommunication Sector

ITU-T—ITU Telecommunication Standardization Sector

JISC—Joint Information Systems Committee

LAN—local area networks

LPS—Liberty People Service

MIT—Massachusetts Institute of Technology

OASIS—Organization for the Advancement of Structured Information Standards

PDA—personal digital assistant

PDP—Policy Decision Point

PEP—Policy Enforcement Point

PKI—Public Key Infrastructure

PSP—provisioning service point

PST—provisioning service target

RA—requesting authority

RACF—Resource Access Control Facility

SAML—Security Assertion Markup Language

SDOs—standards developing organizations

SGs—study groups

SGML—Standard Generalized Markup Language

SIM—Sun Identity Manager

SOA—Service Oriented Architecture

SOAP—Simple Object Access Protocol

SOX—Sarbanes-Oxley Act

SP—Service provider

SSO—Single Sign-On

SPML—Service Provisioning Markup Language

STS—Security Token Service

TLS—Transport Layer Security

TM—Trusted Module

TSB—Telecommunication Standardization Bureau

S/MIME—Secure Multipurpose Internet Mail Extension

SAML—Security Assertion Makeup Language

SIGs—special interest groups

SPML—Service Provisioning Markup Language

SSL—Secure Socket Layer

TLS—Transport Layer Security

USIM—Universal Subscribers Identity Module

WS—Web Services

WS-Federation—Web Services Federation

WS-Policy—Web Services Policy

WS-Security—Web Services Security

WS-Trust—Web Services Trust

WSC—web service consumers

XACML—Extensible Access Control Markup Language

XML—Extensible Markup Language

ABOUT THE AUTHORS

Dr. Anat Hovav is an associate professor at Korea University Business School in Seoul, South Korea. Dr. Hovav holds a Ph.D. in Management and Information Systems from Claremont Graduate University and has over fifteen years of industry experience in information systems management and strategic planning. Her research interests include the socio-technical aspects of organizational information security, risk assessment, Internet standards, and electronic scholarship. Anat Hovav has published in internationally refereed journals such as: *Information Systems Research (ISR), Communications of the ACM, Computers & Security, Information Systems Journal (ISJ), Information Systems Management (ISM), Advances in Computers, Communications of AIS (CAIS), Information Systems Frontiers, Information Systems Security Journal,* and *Risk Management and Insurance Review*. Dr. Hovav is the program chair of the Annual Information Security Conference held in Las Vegas and has presented her work internationally in academic and industry conferences and workshops.

Ron Berger is a doctoral student in Regional Information, College of Agriculture and Life Sciences, at Seoul National University, Seoul, Korea. He obtained his BS in Forest Resources Management from Humboldt State University, Arcata, CA, and an MA in Environmental Education and Conservation from Rowan University, Glassboro, NJ. He has extensive international work experience in industrial agricultural management and as an instructor in Seoul, Korea. His research interests are social networks, and supply chain management, organizational structure and technical innovations in agriculture.

Communications of the Association for Information Systems

ISSN: 1529-3181