Identity Management: Setting Context

Joseph Pato
Trusted Systems Laboratory
HP Laboratories Cambridge
HPL-2003-72
April 8th , 2003*

E-mail: joe.pato@hp.com

identity management, trust, security, privacy

Identity Management is the set of processes, tools and social contracts surrounding the creation, maintenance and termination of a digital identity for people or, more generally, for systems and services to enable secure access to an expanding set of systems and applications.

This note provides an overview of the issues and offers a model for considering architectural elements of an identity management solution.

* Internal Accession Date Only Approved for External Publication
To be published in the Encyclopedia of Information Security, Summer/Fall 2003

Identity Management: Setting Context

Joseph Pato
Trusted Systems Lab
Hewlett-Packard Laboratories
One Cambridge Center
Cambridge, MA 02412, USA
joe.pato@hp.com

Identity Management is the set of processes, tools and social contracts surrounding the creation, maintenance and termination of a digital identity for people or, more generally, for systems and services to enable secure access to an expanding set of systems and applications.

Traditionally, identity management has been a core component of system security environments where it has been used for the maintenance of account information for login access to a system or a limited set of applications. An administrator issues accounts so that resource access can be restricted and monitored. Control has been the primary focus for identity management. More recently, however, identity management has exploded out of the sole purview of information security professionals and has become a key enabler for electronic business.

As the richness of our electronic lives mirrors our physical world experience, as activities such as shopping, discussion, entertainment and business collaboration are conducted as readily in the cyber world as in person, we begin to expect more convenience from our electronic systems. We expect our personal preferences and profile to be readily available so that, for example, when we visit an electronic merchant we needn't tediously enter home delivery information; when participating in a discussion, we can check the reputation of other participants; when accessing music or videos, we first see the work of our favorite artists; and when conducting business, we know that our partners are authorized to make decisions. Today, identity management systems are fundamental to underpinning accountability in business relationships; providing customization to user experience; protecting privacy; and adhering to regulatory controls.

1 What is Digital Identity

Identity is a complicated concept having many nuances ranging from philosophical to practical. For the purposes of this discussion, we define the identity of an individual as the set of information known about that person. For example, a person's identity in the real world can be a set of names, addresses, driver's licenses, birth certificate, field of employment, etc. This set of information includes items such as a name which is used as an *identifier* – it allows us to refer to the identity without enumerating all of the items; a driver's license or birth certificate which are used as an *authenticator* – they are issued by a relevant authority and allow us determine the legitimacy of someone's claim to the identity; a driver's license which is used as a *privilege* – it establishes the permission to operate a motor vehicle.

Digital identity is the corresponding concept in the digital world. As people engage in more activities in the cyber world, the trend has been to link the real world attributes of identity with an individual's cyber world identity giving rise to privacy concerns.

2 Elements of an Identity Management System

Identity management solutions are modular and composed of multiple service and system components. This section outlines components of an example identity management architecture illustrated in figure 1.

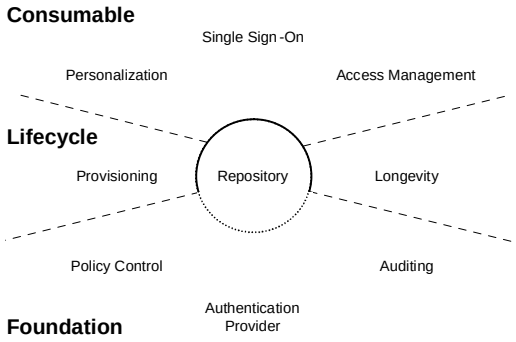

Figure 1. Identity Management System Components

2.1 Identity Management Foundation Components

- **Repository** – At the core of the system is the logical data storage facility and identity data model which is often implemented as an LDAP accessible directory or meta-directory. Policy information governing access to and use of information in the repository is generally stored here as well.
- **Authentication Provider** – The authentication provider, sometimes referred to as the *identity provider*, is responsible for performing primary authentication of an individual which will link them to a given identity. The authentication provider produces an *authenticator* – a token which allows other components to recognize that primary authentication has been performed. Primary authentication techniques include mechanisms such as password verification, proximity token verification, smartcard verification, biometric scans, or even X.509 PKI certificate verification. Each identity may be associated with more than one authentication provider. The mechanisms employed by each provider may be of different strengths and some application contexts may require a minimum strength to accept the claim to a given identity.
- **Policy Control** – Access to and use of identity information is governed by policy controls. Authorization policies determine how information is manipulated; privacy policies govern how identity information may be disclosed. Policy controls may cause events to be audited or even for the subject of an identity to be notified when information is accessed.
- **Auditing** – Secure auditing provides the mechanism to track how information in the repository is created, modified and used. This is an essential enabler for forensic analysis – which is used to determine how and by whom policy controls were circumvented.

2.2 Identity Management Lifecycle Components

- **Provisioning** – Provisioning is the automation of all the procedures and tools to manage the lifecycle of an identity: creation of the *identifier* for the identity; linkage to the authentication providers; setting and changing attributes and *privileges*; and decommissioning the identity. In large scale systems, these tools generally allow some form of self-service for the creation and ongoing maintenance of an identity and

frequently use a workflow or transactional system for verification of data from an appropriate authority and to propagate data to affiliated systems which may not directly consume the repository.

- **Longevity** – Longevity tools create the historical record of an identity. These tools allow the examination of the evolution of an identity over time.

2.3 Identity Management Consumable Value Components

- **Single Sign-On** – Single sign-on allows a user to perform primary authentication once and then access the set of applications and systems that are part of the identity management environment.
- **Personalization** – Personalization and preference management tools allow application specific as well as generic information to be associated with an identity. These tools allow applications to tailor the user experience for a given individual leading to a streamlined interface for the user and the ability to target information dissemination for a business.
- **Access Management** – Similar to the policy controls within the identity management system foundation components, access management components allow applications to make authorization and other policy decisions based on privilege and policy information stored in the repository.

3 Trends Driving Identity Management

Several trends have combined to drive the need for identity management systems. Consumers, e-businesses, enterprises and governments all see value in the emergence of mature identity management systems. Often the requirements of these communities are complementary, but in some cases conflicting needs raise new issues.

3.1 Consumer Trends

With each new web site a user discovers, consumers finds themselves creating a new digital identity. This proliferation of accounts is tedious both in the work needed to keep information correct and in the need to remember unique account name password combinations. Often this leads to security vulnerabilities such as when consumers choose poor, easy to remember passwords, or use the same password at a collection of independent sites. Consumers are looking for web based single sign-on that allows easy access to a variety of sites.

The emergence of information aggregators for financial services in the late 1990's is evidence that consumers are driven to the convenience of easy access – even at the expense of disclosing some sensitive information to a third party. These aggregators provided a portal which extracted information from the consumer's financial service providers. To access this information, consumers needed to disclose account information and access passwords to the independent aggregator service.

Consumers, however, have demonstrated resistance to the notion of a single universally usable digital identity. The selective disclosure inherent in managing independent identities allows users to maintain different personas for different interaction environments. This is consistent with how people interact in the physical world and is illustrated in figure 2. As a result, consumers are looking for identity management systems that support some degree of anonymity or pseudonymity.

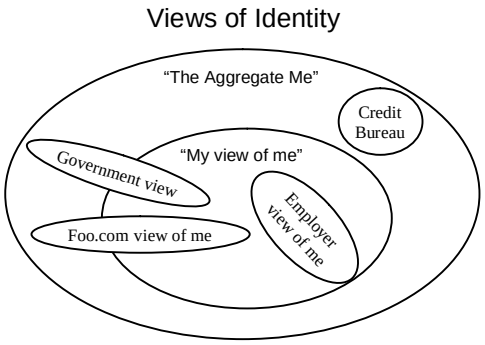

Figure 2. Multiple Views of Identity

3.2 e-Business Trends

Electronic businesses are motivated to please their customers and therefore to deploy the ease of use aspects enabled by identity management systems. Perhaps more importantly, they are also looking to extract direct value from the system. For large conglomerates, an identity management system allows e-businesses to consolidate their relationship with customers – it allows the organization to present a single face to the consumer. Personalization systems allow the business to learn about the consumer and then target advertisement and special offers based on individual history and stated preferences.

3.3 Enterprise Trends

User account and password management has long been a major expense for enterprise IT organizations. Network operating systems and environments have provided some relief, by allowing a single account and password to work on a collection of machines, but this has failed to provide true single sign-on for heterogeneous environments. As enterprises are driven to greater degrees of collaboration with business partners, as they integrate supply chains the number and diversity of systems and applications increases. Enterprises are driven toward identity management solutions that will address heterogeneity issues and allow them to integrate with their business partners. They need systems that will provide for independent administration and that will provide strong accountability for business transactions.

3.4 Government Trends

With the evolution of e-government initiatives, governments share many of the concerns motivating e-businesses. Scale, however, is more of a concern for government organizations – few businesses have a customer base the size of a government's citizenry.

Governments, however, do have some other concerns. Privacy regulations such as the EU privacy directive or US sector specific legislation such as the Gramm-Leach-Bliley act of 1999 or the Health Insurance Portability And Accountability act of 1996 create specific controls on how personally identifiable information can be processed in IT systems. These regulations establish requirements for the privacy policy control component of an identity management system, and impose constraints on how businesses exploit identity information.

4 Models for Deploying Identity Management

Identity management systems are primarily being deployed in one of three models: as silos, as walled gardens, and as federations.

4.1 Silo

This is the predominant model on the Internet today. In this model the identity management environment is put in place and operated by a single entity for a fixed user community.

4.2 Walled Garden

Walled gardens represent a closed community of organizations. A single identity management system is deployed to serve the common user community of a collection of businesses. Most frequently this occurs in business to business exchanges and specific operating rules govern the entity operating the identity management system.

4.3 Federation

Federated identity management environments are now emerging. These include systems like Microsoft's .Net Passport and .Net TrustBridge and the Liberty Alliance Project: Liberty Architecture. The central difference between federated identity systems and walled gardens is that there is no single entity that operates the identity management system. Federated systems support multiple identity providers and a distributed and partitioned store for identity information. Clear operating rules govern the various participants in a federation – both the operators of components and the operators of services who are rely on the information provided by the identity management system. Most systems exhibit strong end-user controls over how identity information is disseminated amongst members of the federation.

5 Identity Management Issues

Identity management systems bring great value to the digital world and federated identity environments in particular hold great promise for widespread deployment. As the distinction between real world identity and digital identity becomes more blurred, however, a number of issues remain to be considered[1].

- **Authenticity of identity.** How is the accuracy and validity of identity information measured and determined? What are the trust services that must be in place to generate confidence in information in the identity management service?
- **Longevity of information.** Do identity management systems provide adequate care to track changes to identity information over time? Do they maintain the necessary artifacts to support historical investigations?
- **Privacy.** Do identity management systems provide adequate controls to preserve individual privacy? Does the system provide adequate support for anonymity and multiple user controlled personas?
- **Identity theft.** Do widespread identity management systems make it easier to perpetrate identity theft or identity fraud?
- **Legal structures.** What protections are in place for the holder of the identity or for the relying party? Do these protections go beyond contractual obligations when digital identity systems are used for interactions that today are limited to the physical world?

[1] For a more detailed examination of issues with large scale identity systems, see the National Research Council's Computer Science and Telecommunications Board report *IDs – Not That Easy: Questions About Nationwide Identity Systems* (2002) available at < http://www.cstb.org/web/project_authentication >.