

THE *Open* GROUP

Identity Management Business Scenario



Copyright © February-July 2002 The Open Group.
All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owners.

All brand, company and product names are used for identification purposes only and may be trademarks that are the sole property of their respective owners.

The Open Group would like to thank all those that have contributed to the scenario through participation in the Workshop, attendance at the Open Meeting, or submission of comments. The views expressed in this Open Group Business Scenario are however not necessarily those of any particular member of The Open Group or any particular contributor to the Scenario.

Management Summary

This Scenario explores the requirements for identity management, the environment within which it must exist, and the implementation architectures that have been proposed for it.

Individuals wish to:

- Publish identity and address information;
- Authenticate for service entitlement;
- Pay for goods and services;
- Manage their own identity information; and
- Manage the identity information of their personal contacts.

Organizations wish to:

- Support these personal objectives within the organization;
- Manage their members' and associates' identity information;
- Have data consistency across distributed identity information stores;
- Manage identity information for people who are mobile;
- Achieve seamless e-client management; and
- Prevent fraud.

Identity Management systems and products are needed to enable individuals and organizations to do these things. But the most important need is for a standard Identity Management framework, within which these systems and products can be designed.

The scenario identifies requirements for this framework and describes several architectural models that are used or have been proposed, and that at least partially meet the requirements.

The X.500 idea of a single universal Directory failed, but the X.500 directory model survives as the basis for the many X.500 and LDAP directories in use today. These are deployed in enterprises and form the core of corporate identity management and role-based access control solutions. Public key technology has not led to the universal system of identification, authorization and trust that had been hoped for, but PKI can be and is being deployed effectively within organizations or between the members of restricted sets of organizations. Third-party identity management systems not based on PKI have been put forward, led by Microsoft's Passport, and including the federated approach of the Liberty Alliance, whose detailed proposal is awaited with interest. A standard specific format for representing identity information has not yet emerged, but XML is emerging as a general format within which individual formats can be defined for specific applications.

These are the constraints and possibilities within which a framework for Identity management must evolve. This scenario does not endorse or propose a particular architecture or framework. It aims rather to map out the current situation so that the industry can find the way forward.

Contents

MANAGEMENT SUMMARY	3
CONTENTS	4
FIGURES	5
TABLES	5
BUSINESS SCENARIO PROBLEM DESCRIPTION	6
PROBLEM SUMMARY	6
BACKGROUND OF THE SCENARIO.....	6
DETAILED OBJECTIVES.....	8
INTRODUCTION.....	8
OBJECTIVES FOR THE INDIVIDUAL.....	8
OBJECTIVES FOR THE ORGANIZATION.....	10
VIEWS OF ENVIRONMENTS AND PROCESSES	13
BUSINESS ENVIRONMENT.....	13
BUSINESS DRIVERS.....	14
BUSINESS PROCESSES.....	16
TECHNICAL ENVIRONMENT.....	17
TECHNICAL PROCESSES	18
ACTORS AND THEIR ROLES AND RESPONSIBILITIES	19
HUMAN ACTORS AND ROLES.....	19
COMPUTER ACTORS AND ROLES	20
REQUIREMENTS	23
TRUST MODEL.....	23
SUPPORT FOR ROLES	23
ACCESS CONTROL.....	23
DISTRIBUTION.....	24
SECURITY	24
EASE OF MANAGEMENT	24
EASE OF USE.....	24
COMPLIANCE WITH LEGISLATION.....	24
SUPPORT FOR LEGACY SYSTEMS	24
TECHNOLOGY ARCHITECTURE MODELS.....	25
INTRODUCTION.....	25
THE X.500 DIRECTORY	25
CORPORATE IDENTITY MANAGEMENT.....	25
ROLE-BASED ACCESS CONTROL.....	27
PUBLIC KEY INFRASTRUCTURE.....	27
THIRD-PARTY IDENTITY MANAGEMENT – PASSPORT.....	28
FEDERATED IDENTITY MANAGEMENT – THE LIBERTY ALLIANCE	28
IDENTITY INFORMATION FORMATS	29

APPENDIX A: GLOSSARY OF ABBREVIATIONS30

Figures

FIGURE 1 – COMMUNITIES, INDIVIDUALS, AND ROLES 13
FIGURE 2 – THE ENTERPRISE TECHNICAL ENVIRONMENT 17
FIGURE 3 - COMPUTER ACTORS.....20
FIGURE 4 - AN ENTERPRISE IDENTITY MANAGEMENT ARCHITECTURE.26

Tables

TABLE 1 – HUMAN ACTORS AND THEIR ROLES..... 19
TABLE 2 – COMPUTER ACTORS AND THEIR ROLES21

Business Scenario Problem Description

The human experience of IDENTITY has two elements: a sense of belonging and a sense of being separate

- Salvador Minuchin 1974

Problem Summary

Managing identities is a difficult process that can be made easier by the use of technology. But this is not just a matter of developing a piece of technology that people can use to manage identities. There are already a number of products that can help – directories, databases, personal organizers, and smart cards, to name but a few. What is needed is a framework within which these products can work, and within which new products and services can be developed where required.

What exactly do we mean by *identity*? In this scenario, the word is used for an identifier that is held in or presented to computer systems, and that identifies a person. A person can have different identities when working with different systems, or can even have more than one identity when working with a single system, perhaps when working in different roles.

This scenario is just concerned with people. Computers, buildings, etc. have identities too, and their management presents problems that are often similar to those presented by the management of personal identities, but those identities and problems are beyond our present scope.

The Scenario explores the requirements for identity management, the environment within which it must exist, and the implementation architectures that have been proposed for it, so that the industry can find the way forward.

Background of the Scenario

This Business Scenario was developed by the Directory Interoperability Forum of The Open Group in order to ascertain the requirements for Directories to support Identity Management.

The scenario follows the established Business Scenario format (see *Part IV of The Open Group Architectural Framework (TOGAF)* at <http://www.opengroup.org/public/arch/>). It is an appropriate format for describing this kind of problem, although many of the considerations are “personal” as opposed to “business” ones. Some of the section headings may seem a little incongruous from this point of view, but they have been kept deliberately for compatibility with other business scenarios.

The Scenario is largely based on material from two sources:

- The Identity Management Business Scenario workshop held by the UK Regional Chapter of The Open Group in Reading, UK, on December 18, 2001; and
- The Identity Management open meeting presented on January 23 2002 by the Open Group’s Directory Interoperability Forum, Security Forum, Mobile Management Forum, and EMA Forum, with support from the European Forum for E-Business (EEMA).

The Reading workshop was held to develop input for this Business Scenario in accordance with the Business Scenario method. Following the workshop, a presentation of the Scenario was developed and was given at the Identity Management open meeting.

In addition to the presentation on the scenario input, the Identity Management open meeting included presentations from a range of organizations that have requirements for Identity Management, from technology vendor organizations, and from an EEMA member putting forward the individual person's viewpoint. There were also panel sessions at which comments from the audience were discussed.

The scenario also takes account of discussions both within and outside The Open Group that have taken place during the first half of 2002. During this period, Identity Management has very much been a "hot topic", with a number of White Papers published by analysts and by product vendors, and articles appearing on the Web and in the press. In particular, there has been a stimulating series of articles in the NetworkWorldFusion Directories newsletter (see <http://www.nwfusion.com/newsletters/dir/index.html>), which include references to many other relevant papers, and articles.

Detailed Objectives

Introduction

Objectives in a good Business Scenario are "SMART": Specific, Measurable, Actionable, Realistic, and Time-bound. This section identifies "SMART" identity management objectives for individuals and organizations.

"Specific" means that what needs to be done should be clearly defined. The objectives identified here can be clearly defined for any particular individual or organization. For example, an individual needs to keep track of all his or her different identities. For a particular individual, at a particular time, the specific objective might be to keep track of 40 different user ids and passwords.

In many cases, an objective should include a time constraint to be specific. For example, an individual's objective is to be able to find someone's address or 'phone number. But how long should this take? With paper-based 'phone books and other directories, a typical time would be measured in minutes. Electronic information systems should be expected to be quicker, and "Within one minute" was the time-constraint agreed in the Identity Management workshop for this objective. This should be considered an absolute maximum, with times of a few seconds a desirable norm. Individual time constraints are not given for the objectives listed in this section; but the same general constraint applies: within a minute as an absolute maximum, within seconds as the norm.

"Measurable" means that the objectives have clear metrics for success. The objectives listed here are mostly binary: either you are able to pay for goods and services, or you are not.

"Actionable" means that they provide a basis for determining a solution, and "realistic" means that the problem can be solved within the bounds of physical reality, time and cost constraints. Time will tell but, given the will to succeed, the IT industry should be able to deliver real solutions that meet the objectives identified in this Scenario.

"Time-bound" means that there is a clear statement of when the solution opportunity expires. For the objectives identified in this scenario, there is a window of opportunity of about two years. The problem should be solved, one way or another, in 2002-2003.

Objectives for the Individual

Publish Identity and Address Information

Individuals want to be able to tell people who they are and how to communicate with them. This is the purpose of business cards, letterheads, and e-mail signature blocks.

An individual may publish different information to different sets of people. For example, you might use one letterhead for business communications, containing your work address, and another, containing your home address, for private mail.

SMART objectives for an individual include:

- Give identity and address information in electronic form to another individual;

- Make identity and address information available on the web for public access.

Authenticate for Service Entitlement

People often need to prove their identities in order to receive services. In non-IT-based transactions, a driving license or passport is often used for this purpose. Now, there is increasing use of IT-based transactions, especially over the Web. For these, there are various devices that help prove identity – PKI certificates, smart cards, and so on – but the most common method is to quote a user id and password.

Specifically, an individual may wish to:

- Obtain access to a service over the web;
- Log in to a computer service at work.

Pay for Goods and Services

As well as establishing their identities, people often need to pay for goods and services in web-based transactions.

The SMART objective here is to be able to:

- Make an electronic payment.

Manage Own Identity Information

An individual may have a number of different identities for use with different systems. With the growth of web services, the number of identities owned by each person is increasing. You might try to use the same user id and password everywhere, but different companies expect or require different formats (for example, a web service company may use your e-mail address to identify you but your employer may have a company standard of *initial.first_name*). And, for security reasons, you might use different passwords for different purposes.

As the number of identities grows, managing them becomes more and more of a problem. An individual needs to:

- Keep track of all his or her different identities (the number of identities could be from one upwards, possibly to over 100);
- Publish each of those identities and use it to gain access to services and for payment, as appropriate.

Manage Others' Identity Information

Almost everyone has a circle of friends, acquaintances, business contacts, and so on. They need to keep track all these people, so that they can communicate with them when they wish.

Specifically, an individual may wish to:

- Keep track of the identities and contact details of the people that he or she knows or does business with (the number of people could be hundreds or even thousands);

- Find someone's address or telephone number, given sufficient information to identify the person in question.

Objectives for the Organization

Support Personal Objectives Within the Organization

Organizations generally wish to maximize the effectiveness of their members. They therefore want their members to be able to:

- Publish Identity and Address Information;
- Authenticate for Service Entitlement;
- Pay for Goods and Services;
- Manage Own Identity Information; and
- Manage Others' Identity Information

in the context of their activities within the organization.

In many organizations, however, accessibility to different kinds of information is restricted to different groups of people. Not everyone, for example, may be given access to the CEO's home telephone number. The objective to enable people to manage others' identity information within an organization therefore has an important qualification: people should only see information that they are authorized to see.

Manage Members' and Associates' Identity Information

Many organizations wish to manage the identity information of their members and of people associated with the organization (customers and suppliers, for example) on a corporate basis. Depending on the organization, the number of members and associates could be small (less than a hundred) or large (measured in millions).

Specifically, an organization may wish to be able to, in less than 20 minutes:

- Instantiate a new identity, including granting of appropriate access permissions, and including identification but not procurement of equipment and applications needed to support the individual;
- Reverse the process when someone leaves the organization, including revocation of access permissions;
- Change identity records when an individual changes role within the organization.

Achieve Data Consistency

An organization typically has a number of different stores of identity information. There may be duplication between these stores. They may be held in various kinds of IT system, including those regarded by the organization as being "current" technology, and those regarded as being "legacy".

An organization will wish to have 100% data consistency in these stores:

- Between a select subset of legacy systems and all current systems;
- With change propagation time of less than a minute.

Manage Mobile Members

Organizations increasingly have to cater for physical mobility, as members visit different locations and wish to be able to access information and services from wherever they happen to be. In some cases, users are not allocated specific workstations, but must be able to use any workstation within a designated pool.

Specifically, an organization may wish to:

- Be able to set up a workstation for a registered peripatetic user within 1 minute, except where lengthy software downloads are required; and
- Do this without administrator intervention.

Achieve Seamless E-Client Management

In many organizations there are different departments that handle different aspects of the organization's relationships with its customers or clients. Commercial organizations often have separate sales and maintenance departments, for example. Governments have different departments for social security and pensions. Hospitals have different departments for patient admissions and billing.

Departments often have different IT systems which do not interoperate, leading to the client or customer being treated inconsistently by different parts of the organization, or having to give the same information several times over. The issues are organizational and are often to do with integration of legacy systems.

This state of affairs results in considerable client or customer dissatisfaction, leading to calls for "end-to-end management of employees", "single view of the customer", "joined-up government", and so on.

Organizations not only want to present a seamless interface through human contacts, they particularly want to present a seamless interface over the Web.

To achieve a seamless interface, an organization will wish to implement a co-ordinated management system:

- That enables single-owner management of e-clients;
- Where a change made once (on-line) propagates to all back-end systems;
- That adheres to a specific security policy and architecture; and
- That includes a single sign-on authentication system for the web and internal systems.

Prevent Fraud

Fraud is a major problem for organizations that deal with money or other items of value. It is a particular problem for government departments that are charged with spending public money. In the UK, for instance, social security fraud is a political issue, and successive governments have claimed that they will save large amounts of taxpayers' money by reducing it.

Issue 1, 15 July 2002

Management of identities can reduce fraud by, for example, detecting claims from people who are using other people's identities, or inventing identities, or claiming multiple times under the same identity.

The amount of fraud and the potential for reducing it are difficult to quantify. The most successful fraud is undetected, and therefore unmeasurable. Nevertheless, a large organization that is prone to fraud can target to:

- Save \$millions or even \$billions by reducing fraud.

Views of Environments and Processes

Business Environment

The human experience of identity has two elements: a sense of belonging and a sense of being separate. The concept of identity is bound up with the concept of community.

Everyone has a unique identity. But most people belong to several different communities, associated with their work, home and leisure activities. They have different responsibilities, rights and privileges within these different communities. Some of these responsibilities, rights and privileges are personal, others are associated with the roles that they have.

An extended enterprise is a community. Its members include the enterprise employees plus selected people from other, related, organizations, such as business partners. They may also include selected members of the general public: customers, for example.

There is a vast worldwide matrix of communities, individuals, and roles. There are over four billion people in the world, and probably the numbers of organizations and roles are of a similar order of magnitude. A tiny part of this matrix is illustrated in Figure 1.

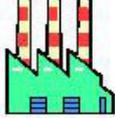
				
	Employee, Salesman		Supplier	Taxpayer
		Owner		Taxpayer, Mayor
		Customer	Employee, Apprentice	

Figure 1 – Communities, Individuals, and Roles

Each individual typically belongs to several communities. The man in the figure works for a company that supplies goods to another company. He is a member of the community that is defined by the company he works for. Within that community he has the roles of “employee” and “salesman”. He is also a member of the community defined by the company that buys goods from his company, and in that community he has the role of

“supplier”. And he is a citizen of his country, having the role in that community of “taxpayer”.

Business Drivers

Individuals and organizations have a number of aims for the management of these identities and their associated responsibilities, rights, and privileges.

Aims of the Individual

Ownership of Identity

Each person wants to be responsible for his or her own identity. People want their organizations to add value to, but not to control, their identity information. And, in Europe at least, government may not allow a large proprietary organization to own people's identities.

Privacy

Most individuals want to keep personal information private, and to restrict access to it to a few known other people. But the desire for privacy and individual dignity must be reconciled with the desire for effective government and with legal needs and national security needs.

Efficiency

Individuals want to maintain their identities in as few places as possible, yet have those identities recognized and accepted by the different IT systems that they use at home, at work, and at play. They want to maintain those identities when visiting different locations and when connected by mobile communications while traveling.

At present, a person may easily have several dozen passwords for a variety of on-line activities, in connection with employment and in personal life. It can be hard to keep track of such a large number of passwords effectively.

Personalized Services

Users want services to react to their specific needs, and are becoming disenchanted with those that do not. To cater for this, systems are becoming personalized, event-driven, and real-time.

Aims of the Organization

Efficiency and Competitive Advantage

Identity management can enable more effective transactions and person-to-person communication. It can improve speed of reaction to change - mergers, reorganizations, and departmental moves. This can help an organization to lower costs, improve productivity, improve business and value chain efficiency, improve customer service, and accelerate time to market.

Identity Management can also enable new services that provide improved quality of experience for customers, giving competitive advantage.

Security

Organizations wish to enable authorized access and prevent unauthorized access to information and services.

In normal commercial operation, there is information that should be protected and kept confidential. Examples are teleconference numbers, executive travel itineraries, contractual and budget information, general day-to-day customer communication, pre-merger communication, event or disaster communications, and legal or accounting information.

Where organizations supply services, they typically restrict access to those services. One reason for doing this is profit: services cost money to provide and may be restricted to those that pay for them. Another reason is to avoid damage to the organization's infrastructure or reputation arising from the activities of "hackers".

Fraud prevention is hard to quantify, but can clearly provide major savings.

An identity and access management infrastructure enables secure business and enhances intranet security. It reduces the risk of improper use of IT systems. It reduces the risk of privacy or other regulatory violations.

An identity and access management infrastructure can also enable secure communication, for example in the form of exchange of strongly encrypted e-mail between business partners.

Mobility

Identity Management should support mobility.

Mobile computing is used within a wide range of areas including utilities, finance, police, healthcare, trucking, construction, manufacturing, field service, emergency services (E911), military, and space exploration. People access services and information from multiple physical locations, using a range of physical devices.

Mobile computing is used because it can minimize time when people are not doing productive work, and maximize the availability of executives for decision-making. It can maximize competitive advantage by timely availability of information, and improve the quality of enterprise information.

The mobile computing infrastructure can keep track of an individual's physical location. This is a requirement in some cases, for example in imposing security policy or in implementing E911 emergency services. It is a key distinguishing feature of mobile computing for identity management. Other distinguishing features are device characteristics (limited display size, bandwidth, etc.) and user expectations: traveling and static users have different expectations.

Mobile computing should provide location transparency: the ability to move from location to location and have your environment move with you. It should also enable a person's rights to depend on their location as well as on their identity. For example, access to some systems may be allowed only to people physically in a particular building.

Consistent treatment of the individual

Individuals like to be treated consistently by the organizations that they deal with, and organizations want to provide consistent interfaces to their clients and customers.

Without management of identity, a business cannot have enduring relationships with its customers, and knowing your customers better than your competitors is a huge advantage in business.

Consistent treatment of the individual may not be easy to achieve. For example, Memorial Health Services in California is responsible for five hospitals. Currently, they have four different inpatient admission systems and many different outpatient admission systems. There are over 80 interfaces between systems, including clinical, financial, and administrative. This makes it impossible to maintain a permanent patient record. This means that: information from previous treatments may not be found when a patient is admitted; payment histories are not maintained; and demographic information may not be consistent. Electronic patient records are an essential tool for clinicians that allows access to patients history online. But they cannot be implemented where there are too many disparate systems.

There are limits to the amount of information sharing that individuals find acceptable. For example, in democratic countries, there is a somewhat polarized position on requirements for shared identity management between different government departments. The terrorist attacks of 11 September 2001 were a big motivator for cooperation, both nationally and internationally. But there is ongoing debate on how the need for effective administration should be balanced against individuals' desires to avoid the "big brother" state.

Conformance to Regulation

Identity management may be needed to enable an organization to meet regulatory requirements.

For example, in the USA the Health Information Portability and Accountability Act (HIPAA) will soon require maintenance of a permanent patient record, with availability of information to carers but security constraints to preserve confidentiality. Hospitals will have to comply to stay in business.

Business Processes

Individual

For an individual, community membership typically involves the following processes.

- **Join Community.** For example: a new employee joins a business, a new customer buys a product on-line, a new citizen is born.
- **Acquire Role.** Within a community, each individual may take on various roles. An employee can be appointed as a salesman, production manager, HR director, or whatever. A citizen can become a voter.
- **Act in Role.** A role can convey rights to access information and services (and, of course, can also include duties). A salesman can access the customer database; the HR director can modify personnel records. A voter may, (in the future, in most places) be able to vote electronically.
- **Give up Role.** Roles are temporary. People quite often change their jobs and other roles.

- **Leave Community.** Employees resign, customers stop buying products, citizens die.

Community

Communities are concerned with the above “Individual” processes, playing a complementary part to that of the individual. They are also concerned with the following community processes:

- **Form.** Companies are founded, voluntary organizations form, government administrative areas are created, and so on.
- **Act.** Each organization carries out a range of activities. Commercial organizations may carry out sales, production and accounting activities, for example. Any of these activities may require management of identities to be effective; for example, effective sales may depend on management of customers’ identities.
- **Merge.** Companies and other organizations sometimes merge. This may imply combining identity management stores; for example, companies that merge may wish to merge their personnel records, their customer databases, and so on.
- **Split.** An organization can break up into two or more parts. There can be de-mergers as well as mergers. This will generally imply that the organization’s identity management stores must be split also.
- **Dissolve.** A company or other organization can be wound up, and cease to exist.

Technical Environment

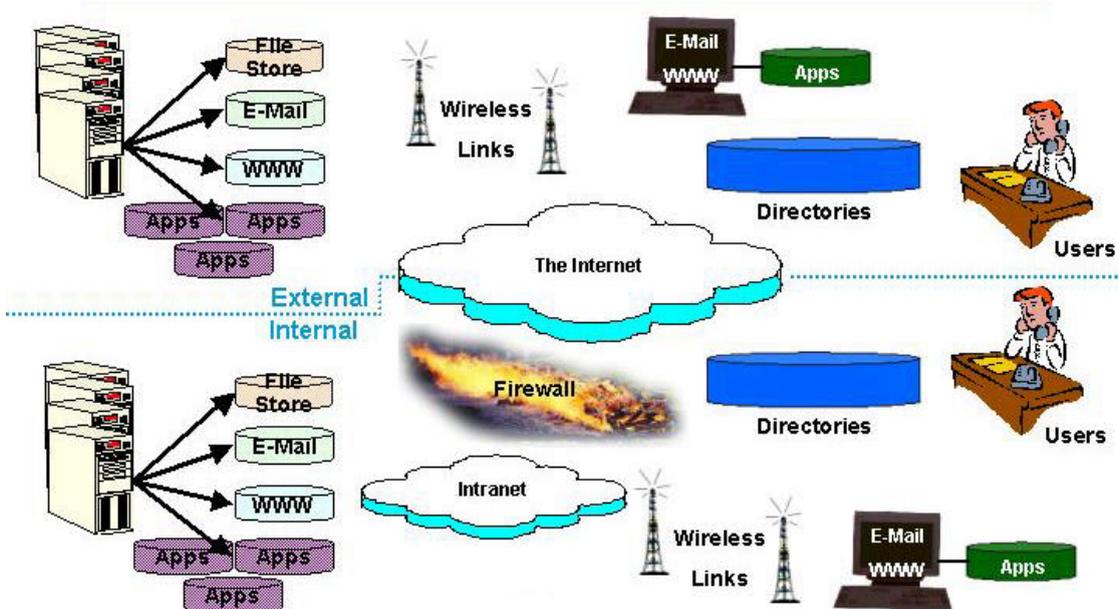


Figure 2 – The Enterprise Technical Environment

Figure 2 is taken from the Business Scenario *The Directory-Enabled Enterprise* that forms part 1 of The Open Group White Paper: Assuring Interoperability for the Directory-Enabled Enterprise. It illustrates a typical enterprise environment, with systems and users within an enterprise Intranet, other organizations' systems and some users communicating through a firewall from across the Internet, and directories holding identity information and other information about users and also about systems.

For reasons discussed in the *Directory-Enabled Enterprise* business scenario, enterprises are finding that the traditional enterprise security model no longer works. The trend is for the hard perimeter enforced by firewalls to disappear, and the distinction between what is inside the firewall and what is outside is disappearing. Everything is becoming more loosely coupled.

At the same time, powerful personal computing platforms are putting power in the hands of the user. A typical personal computer today has a processor with a clock speed of around 1 GHz, hundreds of megabytes of RAM, and tens of gigabytes of disc space. This is much more than enough to store and process all the identity information that an individual could conceivably want or use.

Technology, such as biometrics and smart cards, is emerging that specifically addresses the problem of establishing a person's identity. They provide more reliable alternatives to use of passwords and personal identification numbers (PINs). The choice of method for establishing identity is a question of basic risk assessment in any situation. It may be useful to choose the method of establishing identity on the basis of what is most suited to the application.

Technical Processes

Identity Management involves the following technical processes.

- Create identity
- Update identity information
- Destroy identity
- Archive identity information
- Obtain identity information
- Present identity
- Verify identity
- Signature
- Apply information access control for update and read-access
- Create and maintain identity information stores
- Synchronize identity information stores
- Split and merge stores to reflect organizational changes

Actors and Their Roles and Responsibilities

Human Actors and Roles

The human actors and their roles are listed in Table 1.

Human Actor	Roles
Individual	Has identities. Uses identity and address information of other individuals with whom he or she communicates.
Identity Information Manager	Responsible for identity information within an organization. For example, a Human Resources manager or a member of a security team.
Information Systems Manager	Responsible for design and operation of the organization's communication and information infrastructure.
Developer of tools and applications	Designs and implements Identity Management tools – Perl scripts etc. – and applications.

Table 1 – Human Actors and their Roles

Computer Actors and Roles

The computer actors and their roles are illustrated in Figure 3 and listed in Table 2.

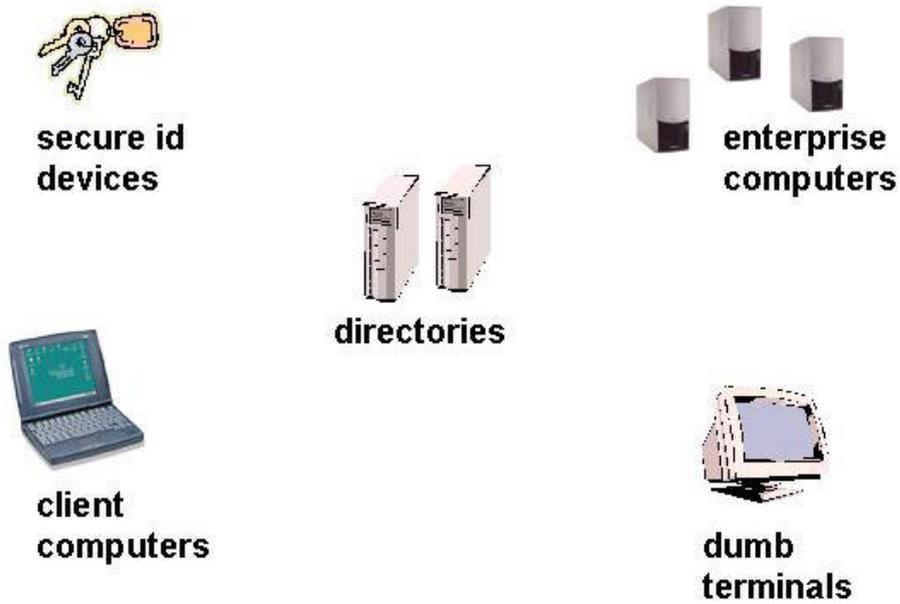


Figure 3 - Computer Actors

Computer Actor	Roles
Secure ID Device	<p>Helps user establish his or her identity.</p> <p>Examples are:</p> <ul style="list-style-type: none"> • Challenge/response devices that generate time-dependant identification codes • Certificate-bearing smart cards • Magnetic stripe cards • Biometric characteristic (e.g. Fingerprint) readers.
Enterprise Computer	<p>Stores information accessed by users.</p> <p>Provides services to users.</p>
Directory	<p>Holds identity information.</p>
Client Computer	<p>Personal information store.</p> <p>Client for access to enterprise information and services.</p> <p>Local application processor.</p>
Dumb Terminal	<p>Provides access to enterprise information and services.</p>

Table 2 – Computer Actors and their Roles

Two of these computer actors – Directory, and Client Computer, need more detailed explanation.

Directories

Directories in the broadest sense are stores that hold identity and related information. They include not only systems that use the ITU X.500 protocols or the IETF Lightweight Directory Access Protocol (LDAP), but also relational databases, flat files, and data stores of other kinds.

Most large organizations have a large number of different systems that are directories in this sense. Their identity information is distributed across them, often with some duplication.

The ITU protocols include server-server protocols that enable different X.500 directories to communicate. A number of *metadirectory* and *virtual directory* products are available that enable organizations to treat a number of disparate information stores as a single directory presenting an LDAP interface.

Client Computers

Individuals use various devices that can store and manage personal information (including identity information), access information and services, or process local applications. They include personal computers (PCs), personal digital assistants (PDAs), and mobile telephones.

Issue 1, 15 July 2002

Identity management features are present in several software applications that run on PCs, including personal directories, personal information managers (which enable individuals to manage diary and other information as well as address information), and office application suites (which also include word processors, spreadsheets, e-mail clients, etc.)

PDA's typically support applications similar to those listed above for PCs, perhaps somewhat restricted in functionality.

Mobile telephones typically include telephone number stores for rapid dialing.

There are synchronization products available to help individuals synchronize information held in different devices. They are not based on formal standards (though the data formats that they use might be considered to be de-facto standards).

But, currently, there is little that an individual can buy "off the shelf" to help synchronize identity information held in a PC, PDA or mobile 'phone with corporate identity stores.

Requirements

Identity Management systems and products are needed to enable individuals and organizations to meet the objectives and fulfill the aims identified in this Business Scenario. But the most important need is for a standard Identity Management framework, within which these systems and products can be designed.

This framework must be standards-based. It must enable the development of commercial off-the-shelf products for identity management.

The framework, and the systems and products within it, must meet the following requirements.

Trust Model

Trust is an important characteristic of identity information. It is not sufficient for a person simply to be given information about another person; the person receiving the information must know how much trust to put in the information itself, and also how much trust may be placed in the person to whom the information refers. Trust is important not just for the individual; trust relationships are very important in the corporate context.

Any framework for identity management must include a viable trust model.

Support for Roles

Identity management should support the association of people with roles, and identity management information should include role information.

Separation of roles should be supported. For example, when an insurance company employee buys insurance from the company his roles as employee and customer must be kept separate. In some cases, it may be a requirement that different roles are filled by different people.

Access Control

Identity Management systems should allow for access to identity information to be controlled, to meet individuals' needs for privacy and organizations' needs for information restriction.

A person may want to restrict particular information to a particular community - for example, may not want work colleagues to know details from personal life. But the individual's wishes are not always paramount.

An organization may need to restrict access to information to protect the privacy of its members, for commercial reasons, or to comply with legislation.

There should be selective control over who (or what) can access or update what information.

Distribution

Information should be available in different locations.

Updates must propagate automatically through distributed stores.

Information obtained in different locations must be consistent.

Security

Identity stores, and clients that access them, should be secure against unauthorized access or modification.

There should be protection against *identity theft*. This is a process by which a criminal knowing a small amount of information about an individual can claim the individual's identity and falsely obtain information or services. The US Federal Trade Commission believes that identity theft is the fastest growing crime in America, affecting approximately 900,000 new victims each year.

It must be possible to follow an audit trail in case of breaches of security or questioned assertions of identity.

Ease of Management

It should be easy for a person to manage his or her identities. The "right thing" should happen without them having to worry about it.

It should be easy for an organization to manage its members' identities. Information should automatically propagate where needed.

As far as possible, individuals should be able to update their own identity information within an organization.

Ease of use

Information Access should be efficient. A person should not have to give the same information several times, and should not have to remember multiple passwords.

Compliance with Legislation

Legislation such as the UK Data Protection act covers (amongst other things) storage of information about individuals by organizations. This legislation differs from one country to another. Money laundering legislation may require tracking of identity information. Identity management products and systems must enable and if possible assist organizations to comply with such legislation.

Support for Legacy Systems

An identity management solution should cater for legacy equipment and applications.

Technology Architecture Models

Introduction

Several architectural models that at least partially meet the requirements are in use or have been proposed. This section gives an overview of them. It does not however propose a particular architecture or framework. It aims rather to map out the current situation so that the industry can find the way forward.

The X.500 Directory

The X.500 Series recommendations were issued by the ITU in the 1980s as a definition of a global directory service for electronic mail. They defined protocols for directory access and inter-directory communication and, most importantly, a general model for directory contents with specific representation formats for certain directory information, including identity information. The IETF later defined LDAP as a directory access protocol for use over the Internet, assuming the X.500 information model and with specific identity information formats based on the X.500 ones.

In the original X.500 concept there would not be a host of different directories. There would be "The Directory" formed by a host of co-operating directory systems all over the world. This universal model for a global directory has failed. But the X.500 directory contents model has survived and become established as the basis for the large number of disconnected X.500 and LDAP directories that exist today.

Corporate Identity Management

Organizations need to create a business context for authenticated identity. They must put in place a flexible infrastructure allowing for linkage between internal systems, the extranet, and the wider Internet. Identity management must be a pervasive part of that infrastructure.

The standards to enable this are only just emerging. Nevertheless, organizations are today deploying systems to meet these needs. An architecture for the identity and access management infrastructure is emerging. Directory services provide the foundation: they are maturing; their focus is moving to directory-enabled services for identity and access management; and the concept of the XML-based registry is becoming important. Identity management systems are extending directories. Provisioning systems are taking on an important role in bridging the gap between portals and enterprise security systems. Web-based access management systems are becoming a popular solution for centralized policy management. Portals provide personalization and are becoming the preferred interface to web-based resources.

There is no standard corporate identity management architecture. Individual enterprises are defining individual architectures to meet their specific needs. An example of such an architecture is illustrated in Figure 4.

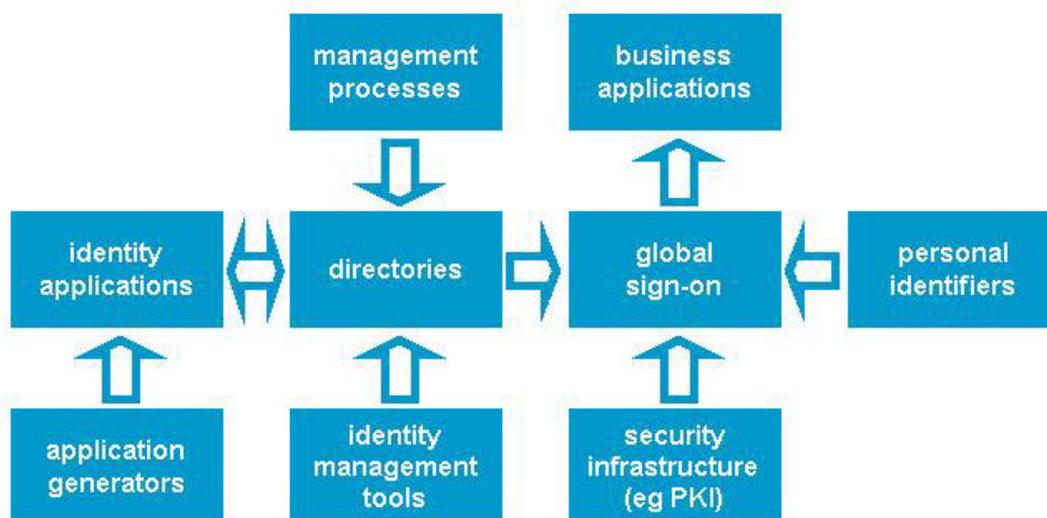


Figure 4 - An Enterprise Identity management Architecture.

Identity information is held in directories, which may include internal-facing directories used by organization members and external-facing directories accessible to the outside world, presenting white and yellow pages services, and with a web interface. A synchronization tool (e.g. metadirectory) enables a number of disparate stores to function as a single directory.

Identity applications and identity management tools help to populate the directories and maintain the information within them. Provisioning-style applications support the process of a new member joining the organization. The definition of such an application requires a form of business process engineering that identifies the permissions, facilities, equipment and services that each new member needs. The resulting application makes the joining process efficient and rapid. Similar applications support the processes of people changing role or leaving the organization.

The directories are operated and updated in accordance with the organization's management processes and policies.

Business-focused applications use the directories. These include web portals and web services applications. There is an application interface for developers. Application generators enable the organization to develop and customize applications to meet its specific needs.

A global sign-on system that uses information stored in the directories supports the business applications. This sign-on system is based on a security infrastructure, such as PKI, and may include use of personal identifiers such as biometric devices and smart cards.

Role-Based Access Control

Role-Based Access Control (RBAC) is a logical architecture used by many organizations to implement control of access to systems and services.

One of the most challenging problems in managing large networked systems is the complexity of security administration. Today, security administration is costly and prone to error because administrators usually specify access control lists for each user on the system individually. RBAC is attracting increasing attention, particularly for commercial applications, because of its potential for reducing the complexity and cost of security administration in large networked applications.

In RBAC, identities are assigned to roles. This can be a many-many relationship. It allows for hierarchical management. Roles are granted privileges.

The benefits of RBAC are that it reduces the number of relationships, reduces changes to access control information, reduces duplication of access control information, reduces management costs, and improves accuracy of access control information. It makes scaling easier, because abstraction avoids the need to deal with minutiae.

RBAC allows enforcement of separation of duties, when a person is not allowed to assume two roles in the same transaction (teller and customer, for example).

Roles should be defined from business policy. This means working with management to define roles and privileges for business processes that may or may not be well defined. In general, a role should be useful for more than one application. Obtaining and managing the role information is a problem when implementing RBAC. The information comes from multiple sources, with different management interfaces, and is often out of date. Updating the information when someone moves from one job to another is a particular challenge. Transitioning from the existing system, and defining roles consistently, are problems also.

Automation is needed for scalability. When automating the role-engineering process, there is a need to delegate and distribute the administration. RBAC should provide for creation of roles by anyone. There should be role engineering for standard roles, but individuals must be able to create ad-hoc roles also.

Public Key Infrastructure

A public key infrastructure (PKI) based on public key encryption technology has long been promoted as the foundation for a universal system of identification, authorization and trust. However, while public key technology is commonly and routinely used in a number of circumstances (for example, for secure Web access), the universal system for identification, authorization and trust has so far failed to appear. Arguably, this failure is one reason for the recent emergence of third party and federated identity management systems.

With PKI, an individual uses a certificate to establish his or her identity to gain access to systems and services. Certificates can also be used to enable secure communications, and for digital signature. A further certificate belonging to a trusted third party establishes the validity of an individual's certificate. A further certificate belonging to another party may in turn establish the validity of this certificate. There can be any number of such levels of validation. The idea is that a small number of top-level certificates could

indirectly establish the validity of any certificate used globally. In practice, this idea has not yet been made to work.

Nevertheless, within organizations or between the members of restricted sets of organizations PKI can be and is being deployed effectively. For example, the Secure Messaging Challenge of The Open Group's messaging forum recently showed how a workable subset of PKI can enable secure communication between business partners.

Third-Party Identity management – Passport

The Microsoft® Corporation launched its Passport initiative to:

- Provide the individual with
 - simplified identity management (“one name, one password”),
 - a safer Internet environment for children (“Kids’ Passport”), and
 - simplified payment;
- And to provide the organization with
 - the ability to extend these benefits to its customers,
 - increased web usage through simplified log-in and registration,
 - improved customer retention by delivering personalized content, and
 - increased sales because of a simplified purchasing process.

Passport works by enabling the individual to register information with the central Passport system that can then be passed to organizations from which the individual wishes to obtain goods or access services. Personal information held in Passport includes: Name; Country/Region State/Territory; ZIP/Postal Code; Time Zone; Gender; Birth Date; Occupation; and Credit card information.

Passport has not at this point become universally accepted as the identity management solution. This is for various reasons, a notable one being the reluctance of the public to trust any single organization to provide a universal identity management solution. This has been reinforced by the fact that security question marks have been raised relating to the specific Passport implementation.

Nevertheless, Passport represents a courageous attempt to solve the problem, and much can be learnt from it.

Federated Identity Management – the Liberty Alliance

The Liberty Alliance (see <http://www.projectliberty.org/>) was founded, at least partly in response to the Passport initiative, to provide similar benefits to Passport, but based on open standards, and through a federated as opposed to a single-supplier approach. It makes interoperability a focus because it respects that other systems will exist and plans to co-exist with them in the marketplace.

Features of the Liberty Alliance approach are that:

- An individual has a single identity, but can have multiple profiles;
- There is a trust model based on “circles of trust”;
- Distributed data stays with the rightful owner;

- There are multiple authenticators;
- There is a delineation between authentication and authorization; and
- The consumer is in control of who can access his or her data.

The Alliance has clearly stated its aims and intentions, but at this point has yet to describe its architectural approach in detailed terms or produce the specifications of its data formats and interfaces.

Identity Information Formats

Interoperability and portability of identity management information is needed within the enterprise, between enterprises, and to integrate with the external public identity infrastructure. It might therefore seem that a standard representation for identity information would be a major step towards the identity management framework that we need. There are indeed a number of identity information representations, but none has yet emerged as the universally accepted standard.

The X.500 recommendations define a standard set of directory attributes for personal information: common name, telephone number, postal address, and so on. Many of these were adopted by the Internet community for use in connection with LDAP. Engineers have gathered in various committees to define a standard set of attributes for "The Internet Person". Several definitions have resulted: the *Lightweight Internet Person Schema* of the NAC, the IMC's *vCard* electronic business card format, and the IETF *inetorgperson* schema, for example. No universally accepted standard definition has however emerged.

This may be because different applications require different sets of personal information. For example, the Enterprise-wide Master Patient Index that is being adopted by hospitals in the US has master permanent patient records, with sub-entries for individual admissions and registrations. It is not possible to identify a core set of information that is common to all applications. Nor is it possible to identify the complete set of information of which any application would use a subset.

Rather than the definition of a single standard information format, the need therefore is for a framework within which individual formats can be defined for specific applications, but with easy manipulation of information and transformation between different formats. This need has driven the development of XML standards such as SAML, XACML, XKMS, DSML, and SPML. When coupled with the web services framework, these standards have significant potential to address the need for interoperability and federation for applications.

Appendix A: Glossary of Abbreviations

DIF	Directory Interoperability Forum
DSML	Directory Services Mark-Up Language
EEMA	European Forum for E-Business (was the European Electronic Messaging association)
IETF	Internet Engineering Task Force
IMC	Internet Mail Consortium
IT	Information Technology
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
NAC	Network Applications Consortium
PC	Personal Computer
PDA	Personal Digital assistant
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SMART	Specific, Measurable, Actionable, Realistic, and Time-bound
SPML	Services Provisioning Mark-Up Language
X.500	A series of recommendations of the ITU relating to directory services
XACML	Extensible Access Control Mark -Up Language
XKMS	XML Key Management Specification
XML	Extensible Mark-Up Language

