# THE *Open* GROUP

# Identity Management

*A White Paper by:*

Skip Slone & The Open Group Identity Management Work Area

A Joint Work Area of the Directory Interoperability Forum, Messaging Forum, Mobile Management Forum, and Security Forum

March, 2004

Identity Management

Document No.:    W041

Published by The Open Group, March, 2004

Any comments relating to the material contained in this document may be submitted to:

>   The Open Group
>   44 Montgomery St. #960
>   San Francisco, CA 94104

or by Electronic Mail to:

>   ogpubs@opengroup.org

# Contents

*Boundaryless Information Flow™
achieved through global interoperability
in a secure, reliable, and timely manner*

## Executive Summary

This White Paper explores key concepts of identity management, places these concepts within their business, personal, and technical perspectives, and proposes a set of steps to be taken by The Open Group to serve as a change agent promoting the resolution of industry-wide impediments to interoperable identity management solutions.

The key concepts explored are trust, authentication, provisioning, authorization, and directories. The issue of trust is explored in terms of its intuitive and historical perspectives, along with the relationship between trust and risk. These concepts are then placed within an information technology (IT) perspective with discussions of IT trust services, delegation of authority, and informed consent. The issue of authentication is explored in terms of identity, relationships, affiliations, profiles, and roles, and is discussed in the context of assuring both verification and timely revocation. Provisioning is the stage at which trust gets translated into the notion of authority, and is explored in terms of a logical lifecycle progression in a business environment. The concept of authorization is explored from the perspectives of managing the permissions associated with IT resources and appropriately integrating this function with identity management. Finally, directories are examined in terms of their roles as data repositories, publication vehicles, and decision points.

Following the discussion of key concepts, this paper examines identity management from various perspectives, including business, security, personal, and technical. The business value of identity management is discussed, both in terms of measuring the investment in identity management and of assessing the risks of either implementing an identity management system or choosing not to do so. In terms of security, identity management is presented as a potential business control that can be implemented to protect business assets. To present the personal perspective, this paper explores various aspects of individual concern, including the role of people individually and as participants in larger social contexts. Finally, technical issues are explored. These issues include the notion of core identity, a framework for identity management, and various issues related to hardware, software, and standardization activities.

The paper concludes by setting forth an action plan by which The Open Group can serve as a change agent for the industry. Proposed actions include the publication of an architecture guide, development of certification programs, and focused coordination with governmental agencies and international standards bodies.

# Introduction

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

*Salvador Minuchin, 1974*

Identity is defined as the quality or condition of being the same; absolute or essential sameness; oneness. Identity is what makes something or someone the same today as it, she, or he was yesterday. Importantly, identity can refer to a thing (e.g., a computer) as well as a person. Things and people can have different identities when working with different systems, or can have more than one identity when working with a single system, perhaps when working in different roles.

A typical large enterprise is operated by people who join as staff (permanent or temporary), contractors, and business partners. These people are assigned roles and act in them. These roles are always "temporary" in the sense that they have no fixed duration. Eventually people either change roles or leave, creating a need for identity information to be actively managed and maintained throughout its lifecycle, frequently across multiple systems.

Globalization of businesses and the increasing integration of information technologies are compounded to make diversity of identity management an obstacle to the continuing development of the enterprise's objectives. To address this, there is a requirement for an integrated approach to identity management to automate, accelerate, and simplify identity creation and maintenance.

Identity Management (IdM) is a convergence of technologies and business processes. There is no single approach to identity management because the strategy must reflect specific requirements within the business and technology context of each organization.

This convergence has drivers from both the business and technology perspective to:

- Enable a higher level of e-business by accelerating movement to a consistent set of identity management standards

- Reduce the complexity of integrating business applications

- Manage the flow of users entering, using, and leaving the organization

- Support global approaches/schemas for certain categories of operational tasks

- Respond to the pressure from the growing numbers of Web-based business applications that need more integration for activities such as single sign-on.

Identity management security is an integral part of many organizations' business strategies.

The integration of directory and identity management is critical to linking individuals and to fulfill diverse and changing functions and roles. Typically, an individual is identified in a directory. A typical directory today contains user credentials and, in some instances, application permissions. Many directories function as the "guard" and policy enforcement point in the enterprise. It is also the starting-point for most single sign-on environments.

# Key Concepts

## Trust

Trust is something we understand at a human level, but not necessarily when it comes to business-to-business relationships or to the technical systems needed to support business relationships. In this section, we discuss a concept of what trust is in a business and technical context, how trust gets translated into the notion of authority, where authority originates, and how it gets delegated. We also explore the relationship between trust and liability, since liability is a business concept that can be objectively measured, and since it is often used in making business decisions. Having established the relationship between trust and liability, we explore contractual aspects of trust and liability, since contracts form the basis of virtually all business-to-business interaction.

### What is Trust?

The dictionary definition of trust is as follows:

Trust: firm belief in reliability, honesty, veracity, justice, good faith, in the intent of another party to conduct a deal, transaction, pledge, contract, etc. in accordance with agreed principles, rules, laws, expectations, undertakings, etc.

### What Trust is Not

It is useful to remember some things that trust is not. Trust is:

- Not transitive (cannot be passed from person to person)

- Not distributive (cannot be shared)

- Not associative (cannot be linked to another trust or added together)

- Not symmetric (I trust you does not equal you trust me)

- Not self-declared (trust me – why?)

### Quotations

"It is good to trust, but better not to."

"Trust, but verify."

*"caveat empto* – let the buyer beware."

### Trust and Identity

Before we talk about managing and using identity in computer systems, we should consider what identity is, and how it is (appropriately) used. The dictionary definition for identity is "sameness of essential or generic character in different instance, in all that constitutes the objective reality of a thing". In this sense, identity is what makes something or someone the same today as he was yesterday. Note that identity can refer to a thing (e.g., a computer) as well as a person.

### Historical Basis of Trust

Confucius told his disciple Tsze-kung that three things are needed for government: weapons, food, and trust. If a ruler can't hold on to all three, he should give up the weapons first and the food next. Trust should be guarded to the end: "without trust we cannot stand". Confucius' thought still holds true today.

From this simple statement, we can deduce that in any business transaction, both parties should start from the assumption that the other party is not trustworthy, then establish whether the other party can be trusted for the purpose of this transaction.

Trust is a notion that has been built up over centuries, based on the simple principle that it is nice to trust someone, but it is better not to because human nature has demonstrated time and time again that if you have something of value then others will want it even if they do not have the wealth or the inclination to pay your price for it. It is therefore your responsibility to safeguard not only what you have, but also what its value is, and to ensure you receive your agreed price when exchanging it.

### Historical Source of Authority

Throughout human history, until the last century or so, people lived and operated in small communities. In such a small close-knit community, if Alice talks to Bob about Carol, Alice and Bob can use Carol's name with assurance that the name identifies the same person to both of them. Also in a small community, there are few secrets so no material information is hidden. Therefore, the name "Carol" carries with it a great deal of information about her. Over this history, the habit developed that a name stands for a person and all of that person's important characteristics (marital status, dependability, credit worthiness, etc.). The sum total of those characteristics amounts to a person's identity.

However, now that we no longer live in such small communities, we cannot use names of other parties as if they are unique and meaningful in this way. We want to be able to do deals with people and organizations we have never met and have little time to get to know at a personal level, over the global Internet.

The ability to describe a person to another person meaningfully – having enough information to be useful (but not so much as to give concern or offense to the person described by invading their personal privacy) – is one of the biggest challenges in on-line identity.

### The Relationship between Trust and Risk

Management of risk and the issue of trust are governing progress in the whole field of e-commerce. They are the critical factors holding back further growth. The continuing development and growth of e-business depends on improving public confidence in using it, raising confidence levels to counter the whole range of security risks and vulnerabilities.

It is fundamental to a business that it will take risk decisions with every business transaction. As a consequence, a business decision-maker needs to be sure that the transaction will be completed to the satisfaction of both parties. Confidence that it will involves a process of gathering information to provide the decision-maker with sufficient information to enable them to make an informed risk decision.

To gather the information needed, the decision-maker often goes to third-party information providers to gather information – references, *bona fide*s, credit checks, etc. – all aimed at

building a confidence profile that the other party is plausible and capable of undertaking the deal involved. The use of third parties in business has been with us for centuries. The third party builds a reputation for delivering good or reliable information on trading companies, sometimes in a general business sense and other times in a niche.

Risk is, of course, based on assessing what the loss might be if something goes wrong, and whether you can absorb that loss if it does go wrong. Thus, we have levels of trust. For a small-value transaction, the degree of confidence in a trust assessment does not have to be large; for a multi-million dollar transaction, the level of trust needs to be very high. The required level of trust depends on your business policies on trust and risk management. A very common risk management approach is staged payments and bank bonds; another is to cover unacceptable financial risk by insurance.

**IT Trust Services**

Technology-dependant businesses need to enable appropriate risk decisions to be made. Trust services can be provided to automate steps in the business process to build trust, checking identity credentials on people and institutions, authenticating sources, etc.

There has been a tendency within the IT community to misrepresent "trust" as a single process at a point in time, whereas trust is a process in itself. Trust is built or destroyed over time. Trust is generally subjective, though it may be supported by empirical information. This has resulted in the user community losing confidence in IT solutions providing a reliable basis for trust.

The delivery of empirical information in support of trust services by electronic means is both practical and necessary for the future growth of e-business. This development should enable more improvements in business process efficiency and better control over the business transactions.

**Delegation of Authority**

The analysis of a business transaction shows that multiple services are used in establishing trust. Some services are delivered by telephone, some by mail, others by reference to a published source of data. There are also services delivered by lawyers, auditors, accountants, notaries, or other professional groups. Members of these groups are trusted to deliver correct information for various reasons, which may be important later in the digital delivery of these services.

A person may decide as a matter of policy or individual case to delegate a trust decision to an automated process, another person, or a third party. However, responsibility for the decision rests with that person. Ultimately, the decisions on trust have to be human ones.

**Informed Consent**

Given the general requirement to enable a business decision-maker to make an informed risk decision, it follows that during any business transaction the decision-maker will want to know what information they need to make the relevant business decision (risk decision). The information will come from a variety of sources. The decision-maker will trust (or not) the sources based on direct and indirect experience. Further, more trust means less perceived risk. More trust may be built by asking more questions of yet more information service providers. Alternatively, more trust may come from seeking information from a more reputable source.

Informed consent is one hallmark of trust between strangers. For example, when I understand a pension plan, a mortgage, or complex medical procedures, and am free to choose or refuse, I express my trust by giving informed consent. (Note that I probably have no prior experience of the person I am trusting.) We give informed consent in face-to-face transactions too, though we barely notice it. We buy apples in the market, we exchange addresses with acquaintances. It sounds pompous to speak of these daily transactions as based on informed consent: yet in each we assume that the other party is neither deceiving nor coercing (we trust them in some limited way). We withdraw our trust very fast if we are sold rotten apples, or deliberately given a false address. So everyday trust is utterly undermined by coercion and deception.

Informed consent is important, but it isn't the basis of trust. On the contrary, it presupposes and expresses trust, which we must already place to assess the information we're given. Should I have a proposed operation? Should I buy this car or that computer? Is this Internet bargain genuine? In each case I need to assess what is offered, but may be unable to judge the information for myself. Others' expert judgment may fill the gap.

## Identity Management and Authentication

In this section we deal with the core concepts of identity management and authentication as follows:

- We start with the fundamental concept of identity.

- We then build out the related concepts of Profiles, Roles, Relationships, and Affiliations.

- We provide an overview of the processes of identity management.

- We explore the critical notion of verification; i.e., the process of establishing identity prior to the creation of an account that can later be used as an assertion of identity. It is noted that verification processes vary widely, in that they can be as simple as allowing a user to choose an unused identifier (e.g., hotmail), or they can be as stringent as requiring personal appearance and possession of government-issued photo identification.

- We discuss authentication, or the process of gaining confidence in a claimed identity.

- Finally, we discuss the process of identity revocation and its ramifications.

### Identity

Identity is the fundamental concept of uniquely identifying an object (person, computer, etc.) within a context. That context might be local (within a department), corporate (within an enterprise), national (within the bounds of a country), global (all such object instances on the planet), and possibly universal (extensible to environments not yet known). Many identities exist for local, corporate, and national domains. Some globally unique identifiers exist for technical environments, often computer-generated.

Unfortunately, many identities now in use are insufficient for the business requirements of most corporations. The most obvious of these is identity for people. As an example, the US Social Security Number is not complete in identifying all employees, nor does it assure uniqueness.

Even in a given context, a person may have multiple identifiers. As an example, in a corporation a person often has a different identifier for payroll systems, email systems, and for various other legacy line-of-business applications.

**Relationships, Affiliations, Profiles, and Roles**

Once identity is established, a wide variety of attributes and objects might be associated to it. Some of these associations might be formal, specific relationships amongst peer objects (e.g., people and bank accounts). Others might be informal, loosely-linked affiliations (often one-to-many and many-to-many) which may change frequently over time. Another link would be people with role-based rules. An example might be that a person as an engineer might have a certain level of signature authority. When that person steps in as acting manager when the manager is on vacation, there will need to be an alternative authority which may be the engineer. Thus, temporary privilege changes could be supported by acknowledging a time window for the additional role.

There is also the situation that a given object might be multi-faceted depending on context. The best examples are people who have multiple profiles (e.g., employee, citizen, personal, consumer, social). Optimally, a person would have a single identity with multiple profiles associated to them that are invoked based on context. However, this raises the conflict of gaining systems consistency and efficiency *versus* potential of exposing personal private information. There are areas where some improvements can occur. For example, consistency within the employee profile would greatly assist system consistency and data integrity within the corporate context. There is no rationale for the corporation for linking that to the personal or consumer profiles. However, there may be advantages from employee benefits (e.g., special purchase programs) that should be considered when a person is in the consumer or personal mode.

**Identity Management**

In many rudimentary implementations of identity management, these subordinate and peer items are often incorporated into the identity object. In a broader context, they should be maintained separately to allow one-to-many and many-to-many links.

**Verification**

Verification is the process of establishing identity prior to the creation of an account that can later be used as an assertion of identity. It is noted that verification processes vary widely, in that they can be as simple as allowing a user to choose an unused identifier (e.g., hotmail), or they can be as stringent as requiring personal appearance and possession of government-issued photo identification.

Requirements for verification are generally based on the sensitivities of the identity itself. In the hotmail example, there is no subsequent privilege granted to the individual. In the stringent example, there is clearly a requirement that the individual is truly recognized as the person they claim to be, leveraging a government validation.

**Authentication**

Authentication is the process of gaining confidence in a claimed identity. Once identities are issued, whenever they are used, there is the requirement that the person using the identity is the person that is qualified to use it. This is to minimize identity theft and is comparable to having to present another identity card whenever you use your credit card.

This requires a process for authentication and an authentication authority. Generally, the identity issuer tends to be the authentication authority. When the only requirement of the identity is uniqueness from other identities, the process of authentication may be quite lax. As the requirements become more stringent, the process evolves from a simple password to two-factor validation and beyond.

**Revocation**

Revocation is the process of rescinding an identity that has been granted. This is a process that must be properly recorded for audit purposes. All systems and processes with which identity has been established must now be notified that identity was revoked. This is required to prevent continued use of the identity under potentially false and insecure contexts. If not done properly, this would open the identity authentication authority to potentially significant liabilities.

## Provisioning and Related Concepts

In this section we introduce the notion of provisioning and its related concepts. Starting with the idea that trust gets translated into the notion of authority, it follows naturally that authorities become the agents of provisioning. This section will discuss the nature and characteristics of authorities, noting that different authorities have different scope. Three key aspects of provisioning will be discussed:

- Account provisioning, which deals with identity-related information associated with individuals, their personal attributes, affiliations, etc.

- Resource provisioning, which deals with business assets such as computers, databases, and applications and the management of permissions associated with those assets

- Account de-provisioning, which deals with the termination of access rights to systems and services and re-allocation of those systems and services

**Authoritative Sources**

Multiple authoritative sources may exist in an organization (HR feeds, systems providing financial data services, directories, etc.). From a best practices and manageability perspective, it is important for an organization to make one authoritative source the main source of identity information (e.g., hiring information, identity's credentials such as user name, social security information, salary). This will help prevent information being fraudulently entered when provisioning an identity into an organization. Receiving, validating, and pushing up-to-date information to the appropriate feeds is important to consistently manage identity information.

**Key Concepts**

Some of the key concepts mentioned above are key, as well, to provisioning.

**Trust**: All provisioning must be based on the concept of a trusted identity. For an identity (e.g., New Employee) that is hired into an organization, trust is usually obtained as part of the HR process. If the identity is external to the organization (e.g., Partner), trust may have to have been already established between organizations. Again, trust in the identity, either by contract or some other means, is essential.

**Delegated Administration**: The concept of delegated administration is important to the smooth functioning of the provisioning or de-provisioning process. There may be numerous

reasons for delegation of administration including vacations, sickness, or just providing back-up so the process is not interrupted. Also, it may be important so that "separation of duty" audit criteria are met.

**Additional Approval**: Organization policy may dictate that, for certain provisioning, multiple or additional approvals are required before an identity is granted access to certain systems and services. For example, if an identity was being provisioned to the role of Vice President, this role may require certain accounts or systems that not only require an approval from the Executive Vice President (direct report) but from the CEO as well.

### Account Provisioning

Account provisioning has a number of core functions that may be performed during an identity's lifecycle.

**Adding an Identity**: Initially, the identity may never have existed. As credentials of the identity are known and collected, the identity is then added, checked against the authoritative source, and the identity is then provisioned to required systems and services.

**Modifying an Identity**: When an identity exists within an organization in which it has been provisioned and a change (e.g., merger/acquisition) occurs, the identity's credentials may require review and adjustment in light of changes to the provisioning system's workflow.

**Deleting an Identity**: Covered under De-Provisioning below.

**Suspending an Identity**: Suspending the identity basically represents the temporary halt of access to systems and services provisioned to an identity. An example of this may be that an identity is on leave or a group of identities, representing a team, is changing from one project to another. The identity(s) are then suspended, thus suspending access to respective systems and services.

**Resuming an Identity**: Once the identity comes back from leave, as stated above, or a new team joins the project, the identity's state will be resumed and appropriate resources will be reassigned.

### Resource Provisioning

An important concept in provisioning is resource provisioning. Resources may be classified as computing and non-computing systems and services. Examples of computing systems and services include disk space on a file server, electronic mailboxes, HR system access, and so on. Examples of non-computing systems and services may be anything from provisioning identities (e.g., employees) to physical assets (e.g., desk, telephone, mobile phone, laptop).

Resource provisioning is the provisioning of identities to systems and services that the identity has the approved access to use.

### De-Provisioning

The de-provisioning of identity is the termination of the identity that had been provisioned to services and systems. The de-provisioning of an identity includes the possible reallocation of those de-provisioned assets to a pool for provisioning purposes. De-provisioning is critical for organizations to review and assess because accounts that are not de-provisioned in an accurate and (especially) timely manner, leave the organization open to considerable risk.

## Permissions Management and Authorization

In this section we deal with the core concepts of permissions management and authorization. Appropriate use of resources (which are typically business assets) is assured through the management and enforcement of permissions associated with those resources. Resource provisioning is typically the vehicle for management of such permissions. The notion of "permissions" and the term "access control" are commonly (and incorrectly) treated as synonymous. Permission to access is certainly a permission to be managed, but it is far from the only relevant permission. Other permissions include permission to compare, write, modify, create, destroy, execute, copy, print, forward, delegate, purchase, authorize, approve, sell, sublease, assign, transfer, hire, fire, promote, and so forth.

In recognizing the wide array of permissions to be managed, it should be clear that the source of authority (or at least the lines of delegation of that authority) may vary significantly depending on the type of permission. An obvious example would be the permissions associated with payroll data. It is reasonable to assume that an employee would have permission to read his or her salary information, but certainly not to modify it!

The management of permissions associated with access control is typically conducted through the management of access control lists; however, access control lists fall short of being able to express non-access control permissions. Two examples of other mechanisms include attribute certificates and digital rights management.

Permissions are allocated to individuals by an authorization authority in order to authorize the individual to use controlled or protected resources. Permissions are not identity attributes, though they may in some cases be derived from identity attributes. For example, an organization may have a policy that states that all employees shall be granted permission to enter the company's building. This policy is essentially a rule which grants "building entry" permission from the "employee" attribute of an individual's identity. In cases in which permissions are derived from identity attributes, it is important to ensure that changes in identity attributes (employee status, age, etc.) are communicated to the person or system in charge of managing permissions, so that permissions can be revised if necessary.

Authorization authorities may allocate permissions to individuals in ways that are completely unrelated to identity. For example, a ticket booth attendant at a movie theatre is an authorization authority; she grants permission to enter the theatre to anyone who pays her $7.50, regardless of identity.

Generally speaking, the set of permissions managed by an authorization authority will correspond to the set of possible uses of the controlled or protected resources for which the authorization authority is responsible. So, for example, an authorization authority responsible for protecting the documents in a document management system will probably manage a set of permissions like "read", "modify", "create", "delete".

## Directories and their Roles

This section discusses directories and the roles they play in identity management and related concepts. Directories obviously serve a role as a repository for some (but not all) identity and permissions data. This section consists of:

- A discussion of the types of identity and permissions data that are appropriate for reposing

in a directory and, while not defining certain data as out of scope, a discussion of the general categories of data that are often deemed inappropriate for directories.

- A discussion of the role of directories as a publication vehicle, including the publication of truly public data as well as restricted data.

- Consideration of permissions-related directory functions. Directories are often relied upon to make decisions, most notably decisions related to authentication. Enforcement of those decisions is often left to another mechanism, such as an access control module associated with a target resource. Although outside the bounds of what many consider to be directories, file directories are typically the repository of access-related permissions information, and are often integrated with the enforcement mechanisms.

**Data Repository**

The traditional role of directories has been that of a data repository for information that requires frequent access, but is relatively stable in nature. Information normally of a white pages nature (phone number, office location, etc.) augmented by email address, and other common personnel attributes have formed the foundation for today's directory content and usage.

As security has become more important, the directory has also taken on many of the elements necessary to ensure security of data and its communications. Elements like public and private keys, passwords, tokens, X.509 certificates, and other elements relating to data security are now regularly stored in directories.

As the concept of identity management (IdM) has taken hold, the favored repository for identity information, naturally, has turned out to be the directory. This is because much of the information necessary for IdM is already stored in a directory. This directory is often centralized and centrally managed. It is a natural follow-on that directory services will play a major role in the storage, access, and management of IdM.

As mentioned above, traditionally, the directory has been the repository of relatively stable information. The rule of thumb often used was that no more than 20% of the information in a directory should be changing over a set time period. If an item was often changed, it usually was not appropriate to store that item in the directory, but rather in some transactional data store – or even as an application-specific item in some proprietary store. Even though the capabilities of directories in speed of change and speed of access have improved dramatically since the early X.500 implementations, this tradition of not including volatile information in the directory stands today.

For example, if an identity in a certain IdM environment is tied to a wireless device and its location, it is highly unlikely that the device's location information will be stored in a typical directory, because that location information is changing all the time. Likewise, if signal strength happens to be an element of identity, that would probably not be stored in the directory either.

In addition to the types of information mentioned above that are typically found in directories, additional, more IdM-specific information might include entries like:

- Policies that govern and control the management, access, and use of the information

- Roles and the privileges associated with each

- Provisioning logic that ensures proper access – possibly based on a combination of policies and roles

- Relationship information relating to customers, partners, suppliers, etc. used to define levels of trust and federation

and other such information.

IdM, as a ubiquitous, interoperable facility is in its very early stages of development. As it matures, the use of the directory as part of its inherent infrastructure will also grow and mature.

**Publication Vehicle**

As IdM grows and matures, and especially as its use outside of the organization grows, the publication aspects of the directory services underlying the IdM facility will become especially important. This is for two basic reasons:

1. The directory will have to publish information.

2. The directory will have to protect information.

As a publication vehicle, directory technology today is mature and ubiquitous. The Lightweight Directory Access Protocol (LDAP) is ideally suited to access information stored in directories – be they LDAP or X.500. It is a well-understood protocol and there are many tools available to developers for creating applications that will utilize directory information.

The difficulty arises, however, in that area of "protecting" the data. It is only properly authenticated and authorized individuals (or applications) that should have access to appropriate information, especially if that information is used in authentication and authorization; that is, IdM. Today (except in the X.500 protocols) there are no standards for "access controls", the common methodology for protecting directory information.

Even though there is no LDAP standard for access controls, each LDAP server vendor has implemented their own methodology to provide access control to their LDAP directory's data. Some of the vendors have based their access controls on the X.500 model, while others have implemented totally proprietary versions.

As IdM becomes more mature and ubiquitous this may or may not present an interoperability issue. (We are not going to detail it here, but the issue is compounded if replication of directory information is involved as well.)

Publication can be further complicated in inter-organization IdM environments (your partners, suppliers, customers, etc.). How you go about publishing necessary information can take a number of forms. Many organizations elect to create and populate a "border" directory that contains the information necessary to work with other organizations. This certainly keeps both the network and other directory information secure, but has the drawback of requiring some way of maintaining and updating information on a current basis. With good firewall and access controls, however, many organizations are now allowing queries inside and passing results back out. This will become less of a problem with the maturity of the IdM products.

**Making Decisions**

Directories, typically, have not been the "decision-maker" in authentication, authorization, or policy interpretation. They have contained the requisite data, but other applications have taken

that data and rendered an appropriate decision. There are exceptions, of course. For instance, Network Operating System (NOS) Directories such as Active Directory and e-directory do make numerous IdM authentication and authorization decisions based on the ability to match credentials supplied by a user or system with the values (securely) maintained in the directory.

As IdM moves forward, this type of functionality will have to become an inherent capability of all directories – if not explicitly making the decision, the matching of credentials and values returned act as triggers to grant or deny requested authentication or authorization.

This will be compounded, of course, as we move into the area of federation of identities. Not only will the actual information required for federated identity be necessary, but that information will be viewed against policies that may differ from one organization in the federation to another. This will bring up another IdM requirement: Policy interpretation and "matching". (This has already been encountered in the current implementation of the US Federal Bridge Certification Authority.)

Without standards-based access controls and a standards-based policy interpretation mechanism, the "making decisions" capabilities required of IdM will continue to be performed, predominantly, by the application and not by the directory.

**Enforcing Decisions**

As stated in the introduction to this section on directories, it is often other mechanisms, usually associated with the application or resource being accessed, that enforce the authorization required. Separate access controls utilize the results obtained from the directory to provide whatever permissions are available to the authenticated submitter.

However, virtually all directory servers today also implement some level of access control, if only to protect the information contained in the directory. These access controls (except in the case of X.500 directories) are proprietary to the individual directory utilized. Were there to be a standards-based access control mechanism (either for LDAP or, more probably for DSML), the directory infrastructure could take on more of the enforcing role than it does today.

NOS directories do provide for some levels of enforcement by their very nature, but this is in combination with the network infrastructure and the OS. It is becoming increasingly difficult to separate these three elements (exampled by Microsoft's marketing a separate Active Directory/Application Mode, disconnected from the OS).

Most general-purpose directories today do not function as "enforcers", but as traditional repositories – leaving the enforcement to the target application. IdM interoperability, federation, and policy interpretation may force more of an "enforcer" role on the directory technology in order to simplify the process (and management) in the medium term. Concepts such as "Groups", "Roles", etc. could then be much more efficiently utilized.

# Business Value of Identity Management

This section is intended to provide a way of translating the technical aspects of identity management into business terms. Whether consciously or not, all businesses expend resources on identity management. By exposing such expenditures, decisions about them can become conscious decisions. This section explores methods of measuring the investment in identity management systems, and discusses the risks of implementing such systems or of continuing to exist in the absence of such systems.

## Overview

The rapid escalation of threats such as hacking, theft of electronic information, spam, viruses, and worms have demonstrated clearly the need to be able to identify who is sending information and using computer resources, and to be able to check that they are acting within their authority.

How should you choose the right computer technology to help you, and how should it be administered? Should you rely on one of the operating system suppliers to solve the problem? Can you outsource it successfully or must you do it yourself? What is involved in each choice?

The Public Key Infrastructure (PKI) is one technical mechanism that offers a means of authenticating people accessing computer systems, originators of information, and computers themselves. But it is often not the only way of achieving your objectives, and you may find alternative authentication technologies can work better to achieve the business objectives of your business policies and operations.

Business Scenarios are a very effective way to model the issues and identify what factors to take into account before selecting the most appropriate technology, in support of their computer identity and authentication functions and processes.

## The Need to Invest – Why Bother?

It is crucial to know who is using computing resources or what computer is attached to your network and therefore potentially who or what is able to access those resources.

In networked systems it is somewhere between difficult and impossible to know who users are or where they are. The technologies for identifying who is using which computer, who sent an email, who requested a credit card transaction, etc. weren't that secure in the networked services and, as a result, hacking, falsified email, viruses, and so on have become real problems. Lack of control means that anyone using a network may have their files copied, altered, or deleted without them or their system administrators necessarily being aware at any stage.

We have to decide what we need to do and how much we need to spend to give us the right amount of comfort that we are able to control the computer systems sufficiently well to meet the demands set out in our business policies. An essential part of our business policy must be to identify and authenticate the users of our computer systems, and also protect the integrity of the information traveling around and between our computer systems.

## What is Identity in IT Terms?

Identification in a computer system means being able to link a computerized (digital) identifier with or to a specific person or a specific component in a computer system (such as a server). The identifier may be a PKI certificate, or it may be other information already stored in a computer system, such as the secret relationship between an identity and a password, or an encrypted token granting them an authority.

Of course you have to consider what items of identification information you are going to use in order to be sufficiently confident that it identifies the specific person or specific component you wish to allow to use your computer system. Just collecting someone's name on its own is not really valuable; other information is needed. The figure below shows a selection of identification information that might be collected.
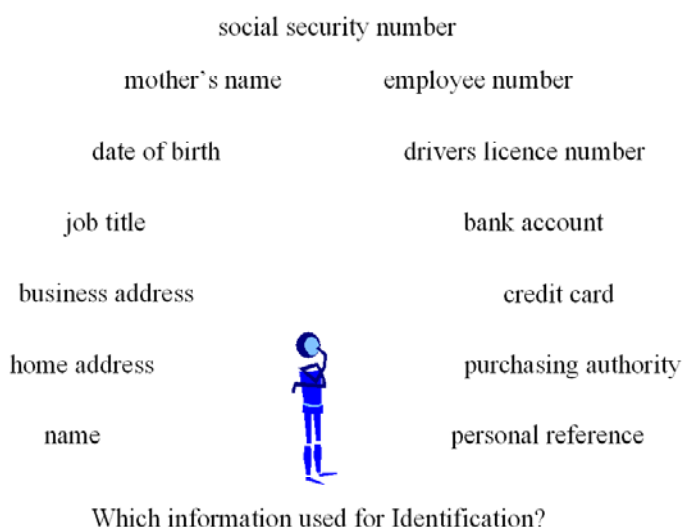
social security number

mother's name            employee number

date of birth            drivers licence number

job title                bank account

business address         credit card

home address             purchasing authority

name                     personal reference

Which information used for Identification?

Figure 1: Identity Information

## Identity and Authentication

Authentication means having some method for checking the computerized identifier being used as the claim of identity back to the specific person or specific computing component to which it was originally linked, and binding that authenticated identity to permissions to perform defined operations on resources in the computer system.

In the case of authenticating an identity, you need to know what items of identification information you are going to check. How successful the authentication is will depend on whether the information that is presented is the information that you were looking for.

## Technologies Available

There is no shortage of technologies that can be used for identifying people. Some of them can be used on their own, while others have to be combined to make them effective. They include Name/Password, Token or Smart Card, and Biometrics. For machine identity, the usual

schemes use either a Unique Identity Code (UID) established as unique by the manufacturer of the machine, or some special name assigned by the systems administrator for that machine.

## Making Informed Choices

Critical to making an informed choice on use of identity and authentication technology is being aware of which technologies are likely to operate most effectively and most cost-effectively in your business.

As a general rule, you will want to put the most powerful authentication where the damage you would suffer if an unauthenticated user gained access would be the greatest. Formal analysis to identify these areas will require modeling to reveal the key operations in your business, and from this prioritizing where the most critical operations are performed and the most sensitive data exposed.

Additionally, the technical and administrative costs to provide and manage the identity and authentication information you require for your selected technology must be included in your assessment.

## The Business Issues

An essential part of any business operations must be to identify and authenticate the users of your computer systems, to a level of confidence that satisfies the criteria defined in your business policies for who (people) and what (other IT systems) is allowed to use each of your information systems.

Clearly your business policies in this regard must first be established. These will dictate what business requirements need to be met to identify and authenticate people or computing components as users of your IT systems. If you have unconnected systems, then the business requirements for each will probably be different and each will require separate consideration. In each case, however, your business policies will define what requirements apply to each IT system.

## Measures of Value and Cost/Benefit Assessment

Reality Check: Specific questions that help to clarify key issues and verify that your requirements do include all necessary considerations should include:

- Who or what do we need to identify, and why?

- Do we need to know their name, or just their authority?

- Apart from their identity, is there some other information to do with them that we need for our business purpose?

- Where is that identification and information going to come from, and if we are not in control of it then who is, and what comeback do we have if they get it wrong?

- What happens if we can't get the identification or information we want when we need it?

- What happens if it is easy for someone else to fake the results we are relying on?

Armed with this information, you can then review:

- How different technologies can provide the specific solutions you need

- What the costs (in both financial procurement and in time and effort to install, set-up, and maintain) are

and therefore which are the most cost-effective for your business.

## Identity and Authentication in System Context

Identity and authentication operate in the context of authorization and access control.

It is important not to confuse these terms. However, they are not essential to the focus of identity and authentication.
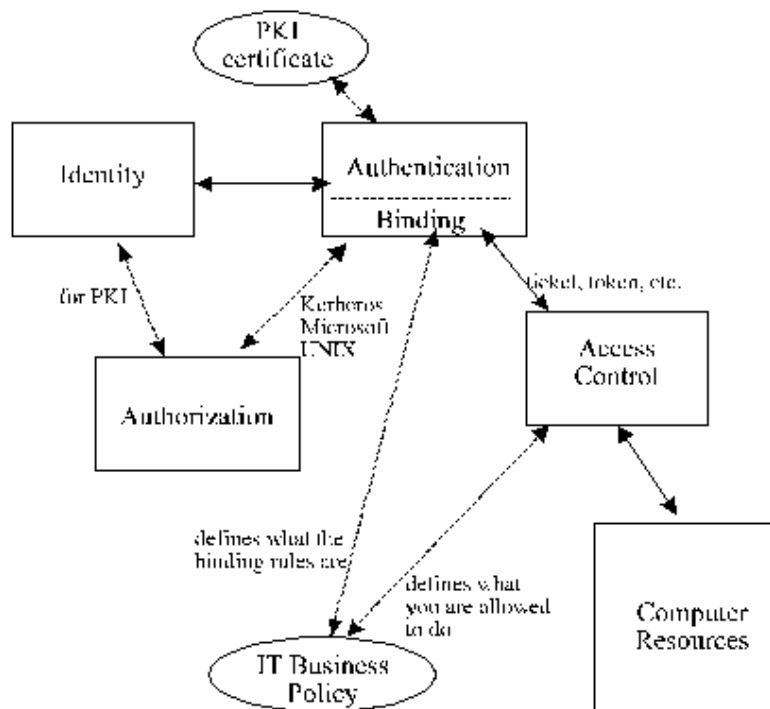
Below is a brief explanation of how they relate:



Figure 2: Identity and Authentication in System Context

**Identity and Authentication**

We are familiar with what identity and authentication mean. Authentication checks the computerized identifier back to the specific person or specific computing component to which it was originally linked. In the case of a PKI certificate, the identification information is included in the certificate. Authentication also binds the authenticated user to what that user is authorized to do, the result being a profile of permissions allowing that user to perform specific operations on resources in the computer system, for example:

- To access data files, with permission to do any one or more of read, write, append, and delete

- To access programs, commands, utilities, etc. to execute them, modify them, etc.

- In networked systems, to access to other computers and the resources within them

**IT Business Policy**

IT business policy provides two sets of information in the system:

- It defines the authentication and binding rules for users

- It defines the operations allowed on computer resources

This information is part of the business policy for how your computer system will be used.

**Authorization**

Authorization in business terms refers to a person or an operational entity having gained the required authority or permissions to do an operation or task.

In computer systems, authorization is where the system administrator or similar authority translates a user's (or a specific group or class of users) permissions to access a designated set of system resources – data files, programs, specific functions and commands, networked facilities, etc. – into computer-recognized form for binding to that user's authenticated identity.

In a PKI environment, authorization information may also be provided to establish identity.

Note that no computer system should be set up to allow an authenticated user to give themselves authorization without being supervised or otherwise validated by a suitably qualified third party.

These principles come from the world of audit controls, where in order to reduce the risk of fraud, no user should be in a position where they can act without anyone else being aware of what they are doing. Unfortunately, many IT systems were not designed with this approach embedded in their control structures, and as a result many existing computer systems have "super-users" who have what is sometimes called "root" powers that give them unconstrained authorization to do whatever they choose.

Such capabilities, without authorization controls, create ideal conditions for hackers.

**Access Control**

Access control refers to the control mechanisms that ensure access and permissions are given to all those who have the required access rights (an authenticated user with the required bindings) to perform specific operations on the resources within that system. This same mechanism denies access to unauthenticated users and to authenticate users if they attempt to perform any operation that they are not authorized to perform.

Systems relying upon access controls usually have lists of the users who are allowed to access the various resources available within it, together with the rights that they have. These lists are referred to as access control lists.

## Technologies used for Identification/Authentication

### People

There is no shortage of technologies that can be used for identifying people. Some of them can be used on their own, others have to be combined together to make them effective. A short list of the principal ones available today, together with some pros and cons, includes:

**ID/Password**: This is the classic log-on identification and has been around for many years. An administrator issues people with individual identifiers (IDs) and an initial password. The user logs on and has to change the password to something new to ensure that it is a secret kept even from the administrator. Sometimes there are rules about how long the password is, letter or number combinations or special characters, how often it has to change, etc. It is cheap to implement and easy to administer. It can be used to enable cryptographic services. It is open to being stolen by many methods, and systems that do not detect too many attempts to use the wrong password are open to computerized attack.

**Token**: Generically, this could mean several things, so we list the commonest meanings, and you should check to see which is actually being proposed.

- A credit card-sized "calculator" type of device. After you have entered an ID/password, the computer system will send you a "challenge" which you have to input on the calculator and it will tell you the correct response that you then enter into the computer. It is used in combination with ID/password in what is called "two factor authentication". This means that you have to know the ID, the password, have the card, and type in the numbers correctly. The token may also need a password or Personal Identity Number (PIN) to get it to work.

- A smart card is used to store secrets, such as an individual's PKI private identity key. The security mechanisms on the card may insist that security operations (digital signing, for instance) can only take place on the card. It may require a PIN to be entered before it can be used, or each time it is used.

**Biometric**: A variety of ways of identifying individuals by means of their physical characteristics are available. Each has its own requirements for registering people, and for implementation. If you intend to use one of these in support of the security requirements of your business process, you should check carefully that you are able to register individuals' biometrics suitably, and have a strategy for dealing with the situation in which the biometric reading device fails to read sufficiently correctly an individual's selected biometric input even though it is the right individual.

Technologies here include:

- Voice

- Fingerprint

- Palm print

- Face

- Eye retina scanning

**Machines**: Machine identification is normally achieved in one of two ways:

- Manufacturer identification – this is where the manufacturer of the machine (computer, smart card, biometric device) provides it with a permanent and unique identification code. This may be a serial number or similar. The manufacturer uses quality control procedures to ensure there are no duplicates issued. Usually a special command to the machine causes it to reveal its identification code.

- User identification – this is where the controller of a machine provides it with a unique identifier. This may not be permanent or unalterable, although there may be operational procedures to prevent unauthorized change. The identity may be in the form of a serial number or it may be the installation of cryptographic keys (which may be PKI keys). A special command can cause the machine to reveal its identity, or information being handled by the machine may be processed with a cryptographic key to prove it came from that machine (or perhaps that it was authorized by the owner of that machine).

# Identity Management as a Business Control – The Security Perspective

Identities working with systems have different permissions and authorities associated with individual systems. These are exercised within management control processes maintaining an appropriate level of checks, balances, and accountability. These ensure that the identity performing the activity is appropriately authenticated and authorized, and that the level of monitoring of those actions ensures adequate accountability. The business control framework associated with identity, authentication, authorization, and accountability is termed "identity management". An audit and appraisal process ensures that the identity management framework is fit-for-purpose and operating as intended.

Identity management in many organizations starts with an appropriate risk assessment to determine the need for identity management controls to properly protect information, applications, and infrastructure as required. These controls set the lifecycle security objectives for creating and maintaining an identity, verifying and authenticating an identity, granting permissions and authorities, monitoring and accountability, and auditing and appraisal of the identity management processes.

An effective identity management standard defines the control objectives required to enforce the organization's policy with regard to identity management security. Such a document provides the linkage between the security policy and other governance structures.

Technical implementation of the identity management standard consists of a framework of business control processes. In the following sections, we provide a sample standard that defines the process and sets objectives for these controls.

The fundamentals of identity management define the control objectives for:

- Identification (the security control process that creates an entity and verifies the credentials of the individual, which together form a unique identity for authentication and authorization purposes)

- Authentication (a security control process that verifies credentials to support an interaction, transaction, message, or transmission)

- Authorization (a security control process that grants permissions by verifying the authenticity of an individual's identity and permissions to access specific categories of information or to carry out defined tasks)

- Accountability (a security control process that records the linkage between an action and the identity of the individual or role who has invoked the action, thus providing an evidence trail for audit or non-repudiation purposes)

- Audit (a security control process that examines data records, actions taken, changes made, and identities/roles invoking actions which together provide a reconstruction of events for evidential purposes)

All the control objectives above serve the requirement to provide an auditable chain of evidence.

In each case in the example standard that follows, the control objectives apply to individuals and roles and their actions on the enterprise infrastructure. The result is the establishment of a baseline identity management standard for identities created, recorded, and managed throughout their lifecycles in applicable directories.

Identity management control processes have an input, one or more control activities, an output, feedback, management monitoring, and an overall audit appraisal activity to ensure that they are fit-for-purpose. The starting point is an individual who is enrolled into an organization and subsequently acts in a function or role in the organization. The individual may be an employee, partner, or contractor, or third party. The output is the appropriate degree of policy enforcement and individual accountability for the business activity. Within the controls, the threats and vulnerabilities constituting the business risk must be addressed and assessed. These include business, legal, and technical aspects.

Many organizations have both vertical and horizontal business structures. These structures are continually forming, merging, acting, splitting, and dissolving. Identity management must play its complementary part in these processes.

A complete identity management architecture has more components than just security. The framework of an identity management solution has several key components:

- Enterprise information architecture
- Permission and policy management
- Enterprise directory services
- User authentication
- User provisioning
- Workflow

An effective standard aims to:

- Build a more responsive and secure identity infrastructure
- Consistently manage identity information throughout its lifecycle across all of the organization's business elements
- Standardize and simplify the interoperability of systems requiring identity information from a multitude of systems and organizations
- Consistently manage user IDs, passwords, PINs, and security tokens
- Integrate business goals with identity processes and policies
- Reduce the burden of administration, lowering operational costs and overheads
- Leverage existing systems investments

An identity management standard should apply to all phases of the lifecycle of an identity in an organization, from initial enrolment (or registration), through maintenance of changes during operational life, to eventual removal and destruction of identity information and associated rights, permissions, and authorities.

## Assessing Risk

**Security Objectives**

- To identify the necessary level of identity management protection and assurances required against unauthorized access to information, applications, and infrastructure elements

- To establish a baseline of risk management for identity management for the infrastructure elements

**Response Control and Baseline for IdM Risk Management**

Line management must conduct an appropriate risk assessment following applicable risk management policy to determine the level of identity management security appropriate to protect their business information, applications, and infrastructure. An example risk assessment methodology is shown at Appendix A.

The identity management risk assessment should identify the appropriate identity security profile required to maintain confidentiality, integrity, availability, and accountability of individual business processes. These inputs will determine whether the identity management security baseline is adequate or whether additional controls need to be put in place.

## Creating and Maintaining Identity

**Security Objectives**

- To ensure that individuals seeking registration for access to infrastructure resources provide reliable and binding evidence of identity before enrolment

- To establish a baseline for creating and maintaining an identity

Identity generally has two forms: that of a distinct individual person and the form of an assigned business role.

Identity must be established as part of an enrolment process to create and maintain an entity identified in a directory. The identification and enrolment process must be sufficiently certain and robust to provide strong confidence in the identity being asserted that the identity is actually "who they say they are". This requires that an individual will need to provide appropriate independent verification of their identity before being permitted to be registered. Where third-party identities need to be enrolled, the identity verification requirements will be specified by contract.

**Response Control**

All identification and enrolment processes developed must be controlled.

This is in order to ensure that at all times it can be demonstrated that a series of strong, evidentially binding, and continuing linkages exist between the verification of identity of the person, the enrolment process, the entry of the person's details into the appropriate directory, and the subsequent assertion of the person's credentials (authorizations, permissions) to infrastructure elements. These controls arise from the need to fulfill a variety of audit, legal, and regulatory requirements.

### Identity Assurance Levels

**Security Objectives**

- To enable individuals to consistently assert electronic identities to all infrastructure elements

- To set standard levels of assurance of identity

- To establish a baseline standard for identity assurance in the infrastructure

**Response Control**

In highly diverse organizations, it is impossible and undesirable to set a single standard identity assurance level applicable to all infrastucture elements and business applications. In order to provide the closest possible match with business and operational security requirements, multiple assurance levels must therefore be accommodated within the infrastructure, directories, and business applications. The risk assessment and development of security risk profiles will determine which level of identity assurance is required and for what purposes within an infrastructure element or business application.

The following classes of identity assurance level will apply across all business entities:

- Level 0: None/Anonymous-level Identity Assurance. Provides minimal assurance of asserted electronic identity. Suitable only for transactions where an error may lead to minimal inconvenience, no financial loss, no distress or damage to reputation, no risk of civil or criminal proceedings, no release of sensitive data to unauthorised parties, no risk to personal safety.

- Level 1: Low-level Identity Assurance. Provides on the balance of probabilities that there is some confidence in the asserted electronic identity. Suitable only for transactions where an error in authentication of identity might lead to minor inconvenience or financial loss, minor distress or damage to reputation, minor risk of release of personal or commercially-sensitive data to unauthorized parties, no risk to personal safety.

- Level 2: Substantial-level Identity Assurance. Provides high confidence in the asserted electronic identity. Suitable for transactions where an error in authentication of identity might cause significant inconvenience, significant financial loss or damage to reputation, significant harm to public interest, risk of civil or criminal violations and be subject to enforcement (including compliance to regulatory, privacy, and data protection requirements), significant release of commercially-sensitive or personally-sensitive material, no risk to personal safety.

- Level 3: High-level Identity Assurance. Provides very high confidence in the asserted electronic identity. Suitable for transactions where an error in authentication of identity might result in considerable inconvenience or financial loss, considerable damage to reputation, considerable distress or harm to public interest, material risk of civil or criminal violations, damaging release of commercially or personally-sensitive material, risk to personal safety.

The US Federal Government has, for its non-Defense agencies, in a similar manner defined a parallel set of identity assurance levels. These are based, in part at least, on the latest Draft

NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.[1]

The four levels of identity assurance were detailed by Bill Burr of the US National Institute of Science and Technology (NIST) in a presentation given in June 2003 at the US Federal PKI Technical Work Group as follows:

- Level 1: Minimal Assurance

- Level 2: Low Assurance

- Level 3: Substantial Assurance

- Level 4: High Assurance

This presentation[2] also details:

- Authentication Technical Model

- Registration and Identity Proofing

- Authentication Protocols

- Agency Process Requirements

for each of the four defined levels.

This policy was codified in the US Federal Register on July 11, 2003.[3]

This process has been taken a step further, with NIST Draft Special Publication 800-63: Recommendations for Electronic Authentication.[4]

## Verifying and Authenticating Identity

### Security Objectives

- To enable an individual to verify and authenticate a claimed identity

- To establish consistent standards of authentication in the infrastructure

- To establish a baseline for verifying and authenticating an identity

Authentication is a process to verify claimed identity (see data origin authentication and peer entity authentication in ISO/IEC 10181-2[5]). This is also defined as a security control that establishes the validity of an originator's credentials, message, or transmission.

### Response Control

Verifying the claimed user name of an individual enrolled in any application or directory is the first essential step towards putting in place effective access control. It provides the first piece of

[1] See http://www.csrc.nist.gov/publications/drafts/draft-SP800-53.pdf.

[2] Bill Burr's presentation is available at http://csrc.nist.gov/pki/twg/y2003/presentations/twg-03-02.pdf.

[3] Available at http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-17634.pdf.

[4] See http://csrc.nist.gov/publications/drafts/draft-sp800-63.pdf.

[5] ISO/IEC 10181-2:1996, Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Authentication Framework. Reprints of ISO standards are usually available for a fee – see: http://www.iso.org.

binding evidence between the identified individual, their subsequent access, and their activity in the infrastructure and business applications. Not all access and applications require the same level of identity authentication. What is essential is consistency of identity assurance at the different levels of authentication.

Authentication can also vary dependent on differences in roles and business scenarios. For example, the rigor of the authentication regime for an individual may be different operating inside or outside an organizational unit's business location.

Authentication is generally performed by an individual claiming a user name and corroborating the claim with some form of credentials or evidence that can be verified by the authenticator. This generally takes the form of one or more of the following:

- Something the user is – a biometric characteristic that can be verified by comparing the characteristic with one created during the identity enrolment process

- Something the user has in his, her, or its possession, usually a token issued during enrolment

- Something the user knows – a shared secret between claimant and verifying authority, such as a password

The strength of the method is related to the business requirement identified in the identity management risk assessment.

## Granting and Maintaining Permissions and Authorities

### Security Objectives

- To ensure that individuals accessing an infrastructure element have been appropriately identified, authenticated, and authorized before access permissions are granted or changed

- To ensure that the method and strength of authorization is appropriate for the requirements identified in the identity management risk assessment

- To establish a consistent baseline for granting and maintaining permissions and authorities

### Response Control

Authorization is a process of granting or changing rights (permissions) and carries with it the scope of authority, which includes the granting of access based on agreed access rights (see ISO/IEC 7498-2[6]). It is a security control that defines and provides the means of granting access after verifying the authenticity of an individual's identity and level of authorization to receive specific categories of information or to carry out defined tasks.

Authorization is directly linked to authentication. Generally, once an entity has been successfully authenticated, the directory provides credentials to IT business services and applications supported by the infrastructure. Consistent and clear levels of authorization can simplify and reduce complexity and costs. Amongst the levels of authorization standards can be a baseline set of permissions to access, read, and modify data.

The authorization process should identify:

6 ISO 7498-2:1989, Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.

- The business activity requirements (and associated necessary permissions and authorities)

- The scope of permissions granted

- The scope of authority

- The limitations

## Suspending and Reinstating Accounts

### Security Objective

- To ensure that an individual account used to access infrastructure elements needing to be suspended or reinstated is subject to the necessary business controls

### Response Control

Suspension and reinstatement of registered accounts are required processes for all infrastructure elements that control access to application systems, networks, and services as part of the identity management lifecycle. These actions may be required for operational, business, or technical reasons (e.g., to temporarily remove access to an application system for maintenance purposes, to manage organizational and role changes, etc.). The control processes developed to manage and operate account suspension and reinstatement must necessarily include actions that notify and seek authorization and approval from business application owners.

## Deregistering and Deleting Accounts

### Security Objective

- To ensure that there is a business control to de-register or delete an individual account used to access infrastructure elements

### Response Control

A clear and managed de-registration of accounts process is required for all infrastructure elements. This is necessary to ensure that identity management controls are properly executed and that registration information is correctly removed from all systems at the end of its lifecycle. Redundant accounts and associated permissions information must be deleted regularly. This will ensure that the risks of unauthorized access to infrastructure elements are minimized at all times.

## Monitoring and Accountability

### Security Objectives

- To ensure that an individual accessing an infrastructure element is appropriately identified

- To ensure that any actions taken by the individual are monitored and recorded in line with the requirements identified in the identity management risk assessment

**Response Control**

There is a requirement to create and maintain a chain of evidence linking the user to the activities they carry out. The extent to which this needs to be carried out will be identified in the identity management risk assessment.

After a user has been identified, authenticated, and authorized, it is essential to establish consistent levels of accountability. The level of accountability provides the evidential chain between individuals and what they have access to and act upon. At the lowest level there is no accountability required to access and view information. At another higher level there is a business need to control not only what is viewed but also modified or presented with a business commitment. Adherence to business policy and legal requirements is paramount and is demonstrated by the chain of evidence available. In addition, accountability will monitor and provide evidence of unauthorized or inappropriate use of the enterprise's services or resources, thus providing a record for both the individual and the business in the event of an incident.

The need for clear lines of individual accountability creates a demand for more information about the organization's businesses and services. Public officials, legislators, and shareholders want and need to know whether business entities are managed properly and in compliance with laws and regulations. Shareholders also want and need to know whether business entities are achieving their objectives and whether they are operating economically and efficiently.

Business managers are responsible for complying with applicable laws and regulations. That responsibility encompasses identifying the requirements to which individuals must comply and implementing systems designed to achieve that compliance.

Business managers are responsible for establishing and maintaining effective controls over the actions of individuals to ensure that appropriate goals and objectives are met; resources are safeguarded; laws and regulations are followed; and reliable data is obtained, maintained, and fairly disclosed.

Business managers are accountable to the enterprise and to shareholders for the resources provided to carry out business activities. Consequently, they should be able to provide appropriate reports on the actions of individuals they are responsible for to those to whom they are accountable.

## Auditing and Appraisal

**Security Objectives**

- To ensure compliance with established policy, procedures, and applicable legislation

- To make an appraisal of identity management performance

**Response Control**

Audit is an independent review and examination of system records and operations in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy, and procedures (see ISO/IEC 7498-2).

Line management is responsible for internal control processes while (internal) auditing provides assurance to business managers and the board of directors that controls are effective and operating as planned. The term "audit" includes both business and performance audits:

**Business audits** include examining business (including financial) statements and business-related performance. Business audits provide reasonable assurance about whether the business statements present fairly the business position, results of operations, and whether financial flows are in conformity with generally accepted accounting principles.

Business audits in relation to IdM determine whether:

• Business information is created in accordance with established or stated criteria

• Individuals have adhered to specific regulatory compliance requirements

• The management control structure over individual reporting and/or safeguarding assets is suitably designed and implemented to achieve the business control objectives

**Performance audits** include cost-effectiveness, efficiency, and business audits.

Economy and efficiency identity management audits include determining:

• Whether the individual is acquiring, protecting, and using their resources economically and efficiently

• The causes of inefficiencies or uneconomical practices

• Whether the individual has complied with laws and regulations

# Key Actors and their Roles

Many different actors play a role in identity management. In an ideal world, their combined efforts will result in the widespread availability of practical, interoperable implementations. This section will identify such actors, providing a description of the role or roles played by each.

### Human Actors and Roles

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

| Human Actor | Roles |
|---|---|
| Individual | Has identities.<br>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.
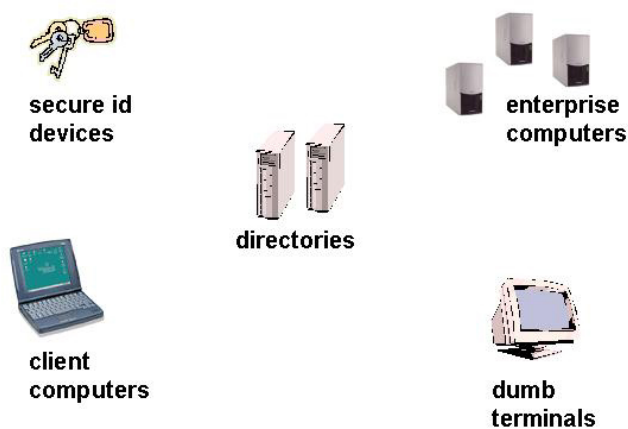
secure id
devices

directories

enterprise
computers

client
computers

dumb
terminals

Figure 3: Computer Actors

| Computer Actor | Roles |
|---|---|
| Secure ID Device | Helps user establish his or her identity. |
| | Examples are: |
| | o Challenge/response devices that generate time-dependant identification codes |
| | o Certificate-beating smart cards |
| | o Magnetic stripe cards |
| | o Biometric characteristic (e.g., Fingerprint) readers |
| Enterprise Computer | Stores information accessed by users. |
| | Provides services to users. |
| Directory | Holds identity information. |
| Client Computer | Personal information store. |
| | Client for access to enterprise information and services. |
| | Local application processor. |
| Dumb Terminal | Provides access to enterprise information and services. |

Table 2: Computer Actors and their Roles

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

**Directory**

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 Computer**

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.

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, email clients, etc.).

PDAs 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.

## Other Actors

There are other actors whose role in identity management should be considered. They are briefly introduced below.

### Platform Providers

Platform providers provide the technical underpinnings of any solution. This includes the hardware manufacturers as well as the operating system providers. Hardware and operating systems need to work in concert to provide the platform on which any solution is deployed. In a heterogeneous environment, operating systems need to work cooperatively with respect to authentication and authorization functions. Operating systems need to provide a consistent interface through which applications can request and consume identity and permissions-related information.

### Application Providers

This is a broad category that includes any provider of application software (and maybe specialized hardware) that provides service to the end user in support of a business purpose. Application providers need to work in concert with platform providers to provide a consistent interface to the user. That is, application providers need to consume the identity and permissions services provided by the platform providers, rather than impose additional identity and permissions interactions on the user.

### Standards Bodies

Standards bodies play a pivotal role in bringing various providers together with one another and with user representatives, and in the forging of Technical Standards that can provide the protocols and interfaces through which heterogeneous implementations communicate.

### Regulatory and Legislative Bodies

Regulatory and legislative bodies play a role in establishing the legal frameworks associated with identity management, most notably in those aspects pertaining to liability and privacy.

### Legal Profession

The legal profession can play a key role in assisting product developers, standards bodies, and users understand the implications of the applicable laws and regulations. By working together with standards bodies and developers, the legal profession can ensure the availability of standards and products that not only work, but that do so within the bounds established by regulatory and legislative bodies. Furthermore, the legal profession can assist lawmakers and regulators in crafting rules that meet both the legal intent and the technical feasibility aspects of identity management.

**Insurance Industry**

The insurance industry has a role to play in identity management with respect to the measurement and management of risks, and through the provision of insurance products that protect both businesses and individuals.

**Industry Analysts**

Industry analysts quite often play a role as change catalysts, by providing a relatively neutral perspective on technical and business issues, by developing analytical frameworks for understanding technical solutions, and by promoting widespread awareness of the issues.

**Privileged Users**

This is a technical role associated with the management of privileged information, such as accounts. Understanding the unique role of such users is essential to the provision of widespread interoperable solutions.

**Individual Users**

Lastly, the subjects of identity management – individual users – must be taken into account. An assessment of individual users should consider them as individuals, with information to provide and be protected, and should consider them as the ones who must interact on a day-to-day basis with deployed solutions.

# Identity Management – The Personal Perspective

Much of this section is derived from and summarizes an earlier Open Group work entitled: Business Scenario: Identity Management.[7]

For comprehensive information on Business Scenarios and how they are used as a tool to link IT architecture and solutions with business problems, see http://www.opengroup.org/togaf/p4/bus_scen/bus_scen.htm.

## The Individual and the Community

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.
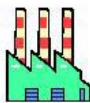
| | | | | |
|---|---|---|---|---|
| | Employee, Salesman | | Supplier | Taxpayer |
| | | Owner | | Taxpayer, Mayor |
| | | Customer | Employee, Apprentice | |

Figure 4: Communities, Individuals, and Roles

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 4.

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".

[7] This document is available at http://www.opengroup.org/dif/projects/im-scen/idmbs_1.pdf.

### General Aims

#### 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, governments 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.

## Specific Objectives

Business scenario "objectives" are described in terms of the acronym "SMART" – Specific, Measurable, Actionable, Realistic, and Time-bound.

#### 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 email signature blocks.

An individual may publish different information to different sets of people. For example, you might use one letterhead, containing your work address, for business communications, 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 Your 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 email 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

# Identity Management – The Technical Perspective

The availability of practical, interoperable implementations depends entirely on the development of a common view of the relevant underlying technical issues. This section addresses such issues, describing in some depth the key technical issues associated with the functions of authentication and authorization, including the secure handling of credentials. Considerable attention is paid to the concepts of core identity and trust in order to derive a common understanding of what information must be conveyed on an inter-system basis to attain interoperability. The section addresses the various points of interface between technical elements, and will address measures designed to protect data independent of where it resides.

## Key Technical Issues

### The Elusive Core Identity

"A rose, by any other name, would smell as sweet."

*– William Shakespeare, who never had to attempt to provide single sign-on across multiple platforms with highly-distributed resource managers consuming non-uniform APIs using inconsistent authorization names; with directory services that are not globally visible; supporting multiple, inconsistent authentication protocols.*[8]

As evidenced by this quote, the essence of identity has perplexed humanity for centuries. People have long asked, and continue to ask: "Is there some essential quality or description that uniquely and unambiguously identifies a thing?" In this section we will explore some of the issues associated with this concept of a "core" identity, and will propose an approach that may at last present a solution to the riddle.

### Names as Identities

Names have long been associated with identity; however, as evidenced by Shakespeare's observation, it is clear that name alone fails to capture the essence of identity. In particular, names alone fail to address the problems of today's identity management environment. Among the more common problems with names are the difficulty of creating unique names that do not conflict with one another, and the tendency of names to change.

A well-understood approach to the problem of uniqueness is to qualify a name by placing it within some context. In a human environment, family names or surnames typically function as the first level qualifier. Failing that, a person's full name is qualified with a physical address or organizational affiliation. If that fails to provide uniqueness, some other attribute is applied. Eventually, the name can be sufficiently qualified to assure uniqueness, albeit cumbersome and a potential source of other problems such as privacy issues.

In the world of interconnected computer systems, name qualification is accomplished through the use of hierarchical names. Examples include the widely deployed Domain Name System (DNS) and the X.500 Distinguished Name (DN), the latter of which is also used for LDAP. Although the syntaxes for these two naming structures are significantly different, the fundamental concept is the same. That is, in each structure, there is a single logical root, below

---

8 As quoted by Jim Hosmer, Lockheed Martin.

which there is a hierarchy of names, and within each structure, global uniqueness is guaranteed by recursively managing uniqueness within the context of each name's immediate superior.

The syntactical difference between the name forms is a consequence of the difference in originally intended purpose of each directory system. DNS was originally designed for naming machines, thus it has a simple naming structure characterized by alphanumeric strings separated with dots. DNS continues to be used primarily for naming machines, although it has evolved to work for other purposes as well. X.500, on the other hand, was originally designed to be a general-purpose directory. Accordingly, the X.500 DN is more complex, consisting of a sequence of Relative Distinguished Names (RDN), each of which consists of one or more attribute type-and-value pairs. The attribute types are used to characterize what type of thing is being named, such as a country, organization, or practically any other type of thing, and the corresponding value distinguishes which particular thing of that type is being named. For example, if naming countries, attribute type-and-value pairs would include c=GB, c=FR, and c=US, to name but a few. Although originally designed to be a general-purpose directory, LDAP today is used primarily as a directory for people. Moreover, the originally envisioned network of registration authorities and root-level structures never got implemented for X.500. Thus, LDAP today is largely implemented as a collection of directories that range from loosely coordinated groups to totally uncoordinated islands. To the extent LDAP directories are coordinated, DNS typically acts as the glue. As such, DNS forms the core of the only globally available directory of both machines and people.

**Directory Names as Core Identity**

The hierarchical nature of directory names allows us to sufficiently qualify a name so as to assure global uniqueness. However, directory names suffer from two significant weaknesses, either of which is enough to disqualify them from further consideration in our quest for a core identity.

The first weakness is the inherent instability of directory names. Since the earliest deployments, directory hierarchies have typically been organized around two key concepts: geography and organization. In DNS, for example, the majority of top-level domains use two-character country identifiers, one for each country of the world, plus a handful of other widely recognized geographical areas other than nation-states. Organizations, on the other hand, make up the bulk of second-level domains, found primarily subordinate to .com, but also very commonly found under the various country domains. Within organizational domains, there is a nearly universal practice of naming sub-domains based on either geography or intra-organizational structure, or both.

Instability in organizational names is introduced primarily through the tendency of organizations to restructure themselves periodically in response to changing business conditions or other variables. Generally speaking, the higher one goes in an organizational name structure, the more stable it is; however, this is no guarantee, as evidenced by the high rate of mergers, acquisitions, and divestitures that occur regularly among publicly traded companies.

Geographical names tend to be much more stable than organizational names, although they are not immune to changes. Unlike organizational names, geographical name instability is more likely to occur at the highest level. The changing maps of Europe and Africa over the past ten or fifteen years speak for themselves in this respect. Although decades seem incredibly long in

contrast to "Internet years", a core identity for such purposes as digital signatures must provide long-term stability.

The second weakness of directory names is the strong tendency of organizations to create asymmetric views of themselves. Externally, organizations have strong incentives to provide a simple structure characterized by customer-friendly interaction, a single point-of-contact, consistency of message, and, when it comes to future products and services, secrecy. Such a view lends itself to shallow, sparsely populated, and relatively flat directory trees that change very little over time. In contrast to the outward appearance, organizations view themselves internally with much more depth and complexity of structure, and this view lends itself to deep, fully populated, highly structured directory trees that can readily adapt to organizational changes. Both of these views are valid, but they wreak havoc on attempts to use directory names as core identities.

### Authorization Identity

Continuing our quest for a core identity, a form of identity worth exploring is the identity used for authorization. The exact form of this identity varies from system to system, as does the precise manner in which it is used. In its most common use, an authorization identity is either a number or string of bits that populates entries in an access control list. Unlike directory names, authorization identities tend to be completely devoid of human semantics, and as such are much more stable. However, authorization identities have other problems that limit their usefulness as a core identity.

The first, and perhaps most difficult problem, is the fact that authorization identities are highly specific to the platforms on which they are used. For example, in Windows, the authorization identity is the security identifier, more commonly known by its acronym, SID. A SID is a variable length binary string used to identify a security principal, which can be a user or group. In UNIX, access control lists are populated with numeric identities known as GID and UID for group ID and user ID, respectively.

### Federation of Identity

Despite the lack of consistent, interoperable identifiers, today's business environment requires that organizations electronically interact with one another. Such interaction can take many forms, including customer-supplier transactions, co-marketing among business partners, and governmental regulation and oversight. The most direct way of enabling such interaction is the establishment and management of separate accounts by which individuals can access and interact with systems. Such an approach is workable on a small scale, but quickly become impractical as the number of inter-organization relationships increases. The difficulty arises for the individual, who has to remember multiple logins, and for the organization, which is faced with a significant administrative burden, and which faces the risk of untimely notification of accounts in need of revocation.

Given the problems of direct account management, organizations are increasingly choosing to federate their identities. In a federated identity environment, accounts are mapped in such a way that a user can access multiple systems, yet only log in once. Behind the scenes, one system authenticates the user, while the target system accepts the authentication credentials. In this manner, federation solves two of the critical problems associated with direct account management. Firstly, it reduces the burden on the user, by allowing a single login to be used across the federated environment. Secondly, it solves the timely revocation problem, in that by

revoking an account at its authentication server, it is effectively disabled throughout the federated environment.

Unfortunately, federation of identity fails to solve all the problems. Authentication identity is not the same as authorization identity. Consequently, even though authentication identity can be federated, authorization decisions, such as access control, still require the management of accounts, in order to establish the authorization identity (such as a SID) used to populate access control lists. Moreover, since the nature of an authorization identity is specific to the platform, and since the prevalent authorization identities are not globally unique, multiple accounts must exist, and these accounts must be mapped to one another. That is, federation of identity does not relieve an organization from the administrative burden of establishing and managing accounts for each individual user.

**Credentials and Protocols**

Authentication involves the presentation of credentials via a communication protocol. The specific form of credential varies with the protocol, and authentication protocols typically do not carry authorization credentials. A notable exception is Kerberos as deployed for DCE and for Windows, the former including an Extended Privilege Attribute Certificate (EPAC), and the latter including Microsoft's Privilege Attribute Certificate (PAC). Without the PAC or EPAC, a server accepting a Kerberos ticket is required to use an out-of-band mechanism, such as a directory query, to build a security context for the user.

A quick survey of other credentials and protocols reveals a variety of non-interoperable, often proprietary mechanisms, each failing in one way or another to solve the complete problem. For example, X.509 authentication credentials can be conveyed using SSL or TLS, but do not provide a viable mapping between authentication and authorization. Web authorization credentials are typically provided as session cookies, which are most often proprietary and non-interoperable. In the web services arena, SAML provides a standardized approach to communicating credentials, yet leaves the specification of those credentials to the implementer.

**Seeking a Stable Authentication/Authorization Identifier**

The Open Group Distributed Computing Environment (DCE) specification included a non-proprietary form of authorization identity, known by two names: the Universally Unique Identifier (UUID), and the Globally Unique Identifier (GUID). For readability, the former term, UUID, will be used for the remainder of this document. The UUID specification included an algorithm for generating binary identifiers in a highly distributed fashion, and provided a very high probability of global uniqueness through the year 3400. Although DCE has diminished considerably in popularity, the use of UUID holds considerable promise, in that its global scope and decentralized nature provide the ability to uniquely and unambiguously identify objects in a persistent, stable manner.

**Convergence Toward a Core Identity**

One of the strengths of the UUID structure is its decentralized nature; however, this is also its biggest shortcoming, in that it lacks any discernable location or scope characteristics. Fortunately, a simple remedy exists: manage UUIDs in pairs, with each pair representing an authority/subject relationship. In this manner, we have the ability to associate globally unique, unambiguous, persistent, non-proprietary identifiers with user accounts. In addition, accounts identified in this manner would explicitly include the identity of the authority responsible for the account. Moreover, by expressing the affinity between an individual and a source of

authority, the UUID-pair identifier satisfies the elusive need to simultaneously convey a sense of belonging and a sense of separateness. Thus, within the context of any given relationship, it is feasible to establish a single core identity for each individual – without sacrificing the very-human concept of identities separate from any particular relationship.

To see how this would work, consider the example that begins with Figure 5. In this example, an account authority is shown, along with two users and a server within its scope of authority. Each entity within this picture, including the account authority itself, has been assigned a UUID. In addition, the account authority holds an account entry for each entity within its scope, and each account entry includes a UUID-pair containing the UUID of the account authority and the UUID of the entity itself.
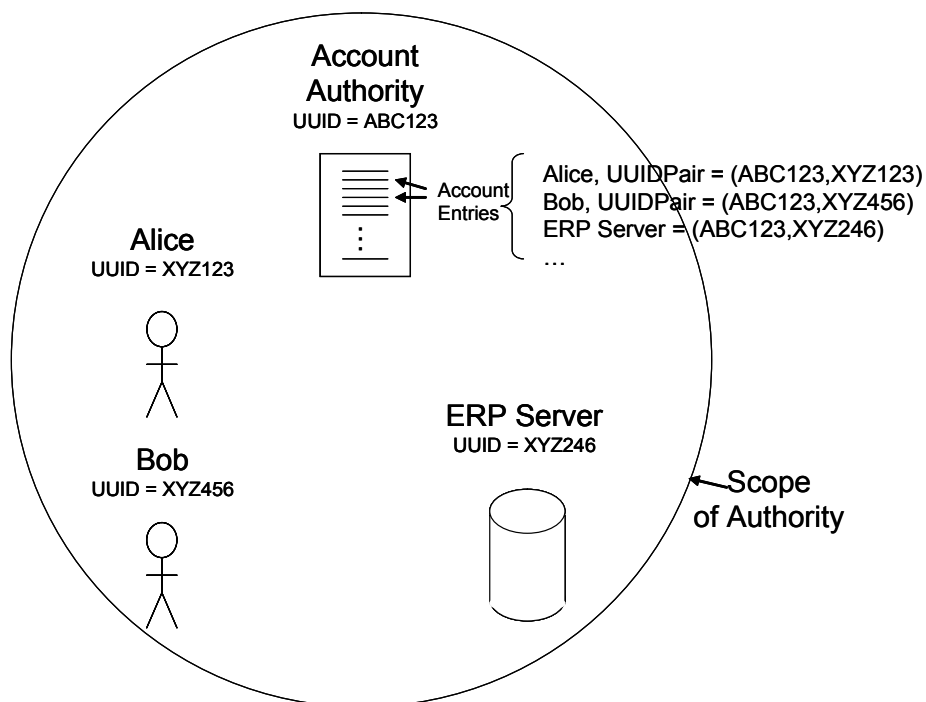


Figure 5: Example Part 1

Continuing the example, Figure 6 depicts a resource on the ERP Server, called "Customer Master", and shows a partial listing of the entries in the access control list that protects the resource. In this example, the entries in the access control list for each identified permission include the UUID-pair for each entity that has been granted that permission. For example, only the account identified by the UUID-pair "(ABC123,XYZ123)" has permission to write to this resource. Notice the last entry under "Read", which illustrates that it is also possible for an access control list to include entries for accounts defined outside the scope of authority for this account authority.
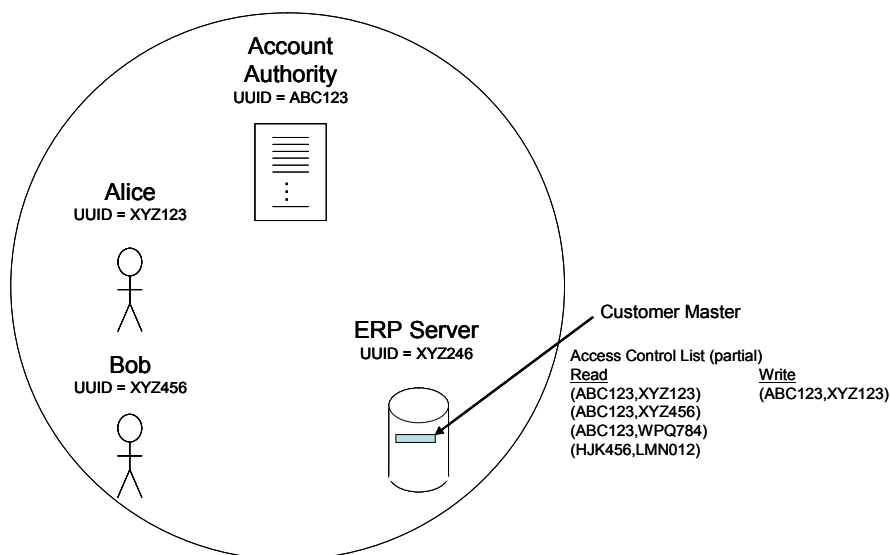


Figure 6: Example Part 2

In Figure 7 we see that Alice has successfully performed a login exchange with the account authority, and is requesting write access to the Customer Master resource on the ERP server. For this to work properly, the credential, such as a Kerberos ticket, that Alice receives from the account authority will include her UUID-pair. When she then passes the credential to the ERP server, it will compare the UUID-pair in that credential with the list of UUID-pairs that have been assigned permission to write to the target resource. In Alice's case, the UUID-pairs in the credential and in the access control list will match, thus she will be authorized to perform the requested action. Note that if Bob requests the same action, his request will be denied because the UUID-pair associated with his account does not match any of the UUID-pairs with write permission.



Figure 7: Example Part 3

The power of this approach only becomes apparent when the scope is extended beyond that of a single account authority, beyond a single operating platform, or beyond the use of a single authentication and authorization me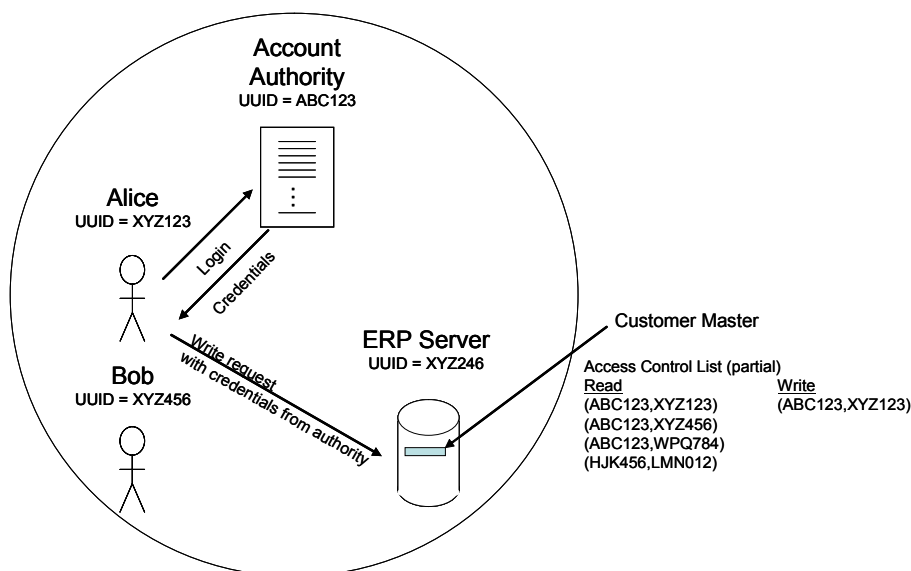chanism. Figure 8 shows an example in which a read request originates from an individual within another enterprise. In this case, a user inside Enterprise B, who has authenticated locally, requests permission to read the Customer Master resource in Enterprise A. It is not shown (and indeed does not matter) what mechanism the user used to authenticate. What is essential to note is that the credential containing the user's UUID-pair, which matches one of the UUID-pairs in the access control list, is passed to the ERP server, which then makes the decision to grant the requested action. In this example, a SAML assertion provided the mechanism for conveying the credential, but again, the mechanism itself is irrelevant.
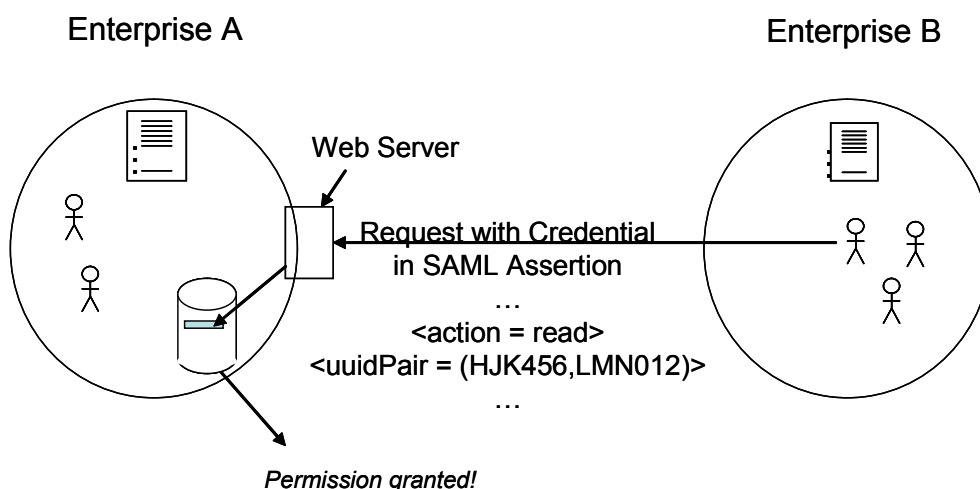


Figure 8: Example Part 4

For simplicity and readability, a number of essential details have been omitted from this discussion. Foremost among these details is the need for a resource manager to decide whether to trust the credential itself prior to making an authorization decision. It is believed that existing technologies, such as digital signatures and related processes for checking revocation status, can be used to satisfy all such supporting requirements.

Wide-scale implementation of UUID-pair as a core identity would permit the industry to move beyond the limitations of currently specified federated identity solutions. As with current solutions, the UUID-pair approach would continue to permit users to log in once in order to obtain a variety of services from multiple providers. In addition, this approach would continue to provide a single point of revocation for identities.

Unlike the current solutions, federation would no longer require the establishment of separate accounts and the resulting inter-account mapping mechanisms. Instead, organizations would follow a two-step approach to establishing trust with an external source of authentication. First, the trusting organization would choose which authorities to trust and whether to trust all individuals authenticated by that source or to trust specific individuals. Second, the trusting organization would populate the relevant access control lists with the UUID-pairs for authorized individuals. The remainder of the solution would be essentially the same as current federation mechanisms.

What has been described to this point is sufficient to establish closed communities of organizations. This capability is essentially what is offered by today's federation solutions. To be globally scalable, however, one challenge remains: the establishment of a mechanism for locating a source of authority for any given identifier. In the following section, we propose a solution for this requirement.

**Source of Authority Location**

As stated earlier, DNS forms the core of the only globally available directory of both machines and people. It stands to reason, therefore, that the ability to leverage DNS to locate sources of authority has considerable merit. From a technical perspective, the solution is fairly straightforward. Although UUID is a binary structure (128 bits long), the widely implemented base64 encoding algorithm can be used to convert the binary string to a "DNS-friendly" text version. The resulting base64-encoded version of the UUID will then fit well within the maximum length requirement for DNS labels. Ideally, DNS resource records registering such UUIDs would be placed in a yet-to-be-established top-level domain. It is expected that the maximum size of such a domain would not exceed the .com domain.

**Trust and Trust Models**

Frustration over Public Key Infrastructure (PKI) failing to be widely adopted is strongly reflected in responses from many organizations. The Information Security (IS) community wanted to take an infrastructure approach but fell short of their ambitions. Thus, many of the concepts that underpin PKI kept surfacing as requirements, possibly via an alternative route.

The following underlying requirements predominate:

- A requirement to associate trust with identity in both procedural (identification) and technical (authentication) terms

- A strong desire to diversify identity issuance and management across the trading community through the use of policy

- A strong desire to increase accountability by having the ability to recognize an individual but retaining the flexibility to provide access (authorization) by role

- A desire to unify registration systems for all

To structure these requirements, we look at:

- The overall goals that an organization seeks from the use of identity, setting them out as a series of architectural principlesThe particular roles (functions) within an identity management framework in which these principles can be implemented, these being six "actors" and describing each in turn

Appendix C contains a sample trust model, including some proposed architectural principles.

## Identity Management Framework

### Introduction

A frequent problem with discussing identity management in a business context is the confusion surrounding what activities need to take place, who should undertake these activities, and who

is relying on the activities having taken place. In short, how is trust defined, implemented, and used?

In this regard, it has been found highly beneficial to bring out these activities as roles or functions within the identity management space, so as to more readily understand each one in the context of the others, and so avoid this confusion.

One advantage of Public Key Infrastructure (PKI) was that many of these activities were well-defined and followed as a matter of course, albeit not always well. While PKI never gained the broad acceptance that the IS community wished for (and the reasons why are not relevant here), the underlying principles remain highly pertinent for implementing identity management. To this end, the well-established PKI-based model is used here as a framework to outline the activities that are required, who undertakes them, whether they are technical or procedural, and what an identity means to a relying party.[9]

It is confidently anticipated that analysis of more recent identity management solutions – such as Microsoft's TrustBridge, the Liberty Alliance's solution, and WS-Federation's solution – will similarly map to this proposed identity management function model.

In the proposed model, six "actors" are identified. In the real world some of these don't yet exist, and others are muddled or confused. These descriptions also diverge from standard IETF views in a few respects, but are provided to provoke thought and discussion.

Not everyone will agree with the labels allocated to these actors. However, it is contended that, in whatever guise, all the actors are required.

They are:

| Identity Management Function | PKI Equivalent |
|---|---|
| Identity Policy Authority (IPA) | Certificate Policy Authority (CPA) |
| Identity Manager (IM) | Registration Authority (RA) |
| Identity Issuer (II) | Certification Authority (CA) |
| Identity Owner (IO) | PKI End-user (EU) |
| Relying Party (RP) | PKI Relying Party (RP) |
| Identity Issuer Auditor (IIA) | Certification Audit Authority (CAA) |

The following sections will now describe these areas.

**Identity Policy Authority**

The Identity Policy Authority is established to define identity. This is a business requirement in each organization. Each identity defined will be associated with a policy that provides the following information:

- **Identity Type**: What this policy is known as; e.g., Highly Trusted.

- **Identity Issuance Policy**: What identity checks are needed to comply with this policy; e.g., Physical Documents provided (listed); Reference Site Checks (Online/Offline, listed); Inspection Mechanism (Face-to-Face, Online, Hybrid).

---

9 It is important to emphasize that this reference to the PKI model is not intended to imply any endorsement of PKI beyond the convenience of using the established PKI-based model as a framework to map to the roles and functions required to implement identity management.

- **Identity Credentials**: What credentials need to be used in conjunction with the identity; e.g., Biometrics, Smart Card, etc.

- **Identity Liability Manager**: Who will take responsibility for reparations in the event of negligence. This will normally be either the Identity Manager or Relying Party. The compliance rules, however, need to be set at this level; in what event the IM is responsible plus levels, etc.

These policies must be published in order that a relying party knows what each policy means in order to take appropriate actions.

The Identity Policy Authority must also ensure that Identity Managers have the appropriate procedures and technologies to enable them to fulfill the policies established. Furthermore, it has an audit role against participating Identity Managers.

In PKI, a Certificate Policy Authority (CPA) performs this role. The CPA exists to devise and offer one or more Certificate Policies. Each Certificate Policy contains details of qualifying criteria and key procedural stages, plus a definition of the resultant certificate contents.

**Identity Manager**

An Identity Manager exists to accept identification information, and in conformance with the terms of Identity Policies, to request that an identity is issued to the Identity Owner. This activity is typically performed by an HR department or a Chief Information Officer/Administrator. The Identity Manager may keep copies of identifying information for audit purposes, and may publish all or part of that information by agreement with its customers/subscribers.

An Identity Manager responds to identity management requests, such as name or address changes, and may act as an intermediary between the Identity Owner and Identity Issuer where an element of non-automatic dialogue is required. Most likely, an Identity Manager will provide some form of directory look-up or address book service to its customers; this is not required for validating identity – that service is provided by the identity issuer.

For flexibility reasons, the Identity Manager may take on the role of "consolidator" of identity services performed on its behalf by delegating tasks to other service providers. For example, providing partial identity information such as credit checking, or it may provide specialized identity management at a place geographically convenient to the end-user; for example, in the workplace. Commercial and shared liability agreements may bind the participants, but it is the responsibility of the Identity Manager to police adherence to policy, as it is answerable to the Identity Policy Authority.

In PKI, the Registration Authority (RA) fulfills this role. An RA performs the normal tasks of an Identity Manager and passes requests for public keys to be signed by one or more Certification Authority (CA). The RA may also provide consolidated certificate revocation information for its customers from a variety of CA sources.

Adherence to the terms of Certificate Policies (CPs) will be audited periodically by the originating Certificate Policy Authorities (CPAs). However, a CP may not contain the complete details of an RA's offering with respect to a particular CP, and so an RA may need to provide additional documentation and details – "service differentiators" – to its customers; for example, Service Level Agreements.

**Identity Issuer**

An Identity Issuer issues identities at the request of one or more Identity Managers. It links a real-world identity to a digital identity. This is largely a technical operation and the separation marks the demarcation between customer-focused process within the Identity Manager and high levels of technical expertise required to properly secure an issued identity. Additionally, there may be considerable gains to be made from economies of scale by separating tasks in this manner.

Identity issuance may cover all aspects of identity from a simple user name and password through to a biometric token.

Note that within the European Union a Qualified Digital Signature Certificate must be issued by a licensed identity issuer.

In PKI, this role is performed by a Certification Authority (CA), which exists to accept public keys and sign them to form X.509v3 certificates.

In the case of encryption certificates, it may optionally choose to publish these to a directory. It may optionally choose to keep a history of the private encryption keys issued to a particular subject (e.g., a person). Public Signature Certificates are not usually published in a CA directory.

The CA is not responsible for establishing the identity of a keyholder, except insofar as this information may be useful for charging for its services, but it must be assured that the keyholder holds the corresponding private key.

A CA responds to certificate management requests, such as automatic key rollover and key recovery, and these requests may originate from an RA or directly from an end-user depending on commercial agreements.

A CA also compiles and makes available certificate revocation information either to an RA or directly to an end-user depending on commercial agreements.

CA machinery is highly secure. The small amount of human intervention required to keep the system healthy is mostly technical, and highly specialized.

**Identity Issue Auditor**

The Identity Issue Auditor establishes the technical and operational rules for all Identity Issuers within its domain. The extent and jurisdiction of the domain may be determined by Government, by commercial groupings, or by individual organizations.

These technical and operational rules provide extensive standards with which Identity Issuers must comply in order to operate within that domain. Additionally, the Auditor may require detailed and confidential information about an Identity Issuer's operation.

For PKI, the audit process is often performed as follows: a CA devises and agrees a Certification Practices Manual with a Certification Audit Authority and publishes a Certification Practice Statement for relying parties, each document describing (with appropriate emphasis and detail) how it goes about its business. The detail it contains is such that a CAA audit can assure the governing body of its domain to a high level of confidence that a CA is providing a safe and reliable service to its customers.

A CA is periodically audited against these documents by a Certification Audit Authority. Optionally, the CPS may additionally be of interest to a consumer watchdog group.

**Identity Owner/End Entity**

The identity owner is the individual making use of an electronic identity to achieve some task or purpose. Frequently this is at the request of the relying party who requires some form of accountability to confirm an action. In business model terms, it is either the IO or the RP who is expected to pay the costs of the IM, II, and IIA, and in practice the decision between the IO and RP resolves down to which gains the greatest benefit. More often than not, the IO finds little reason to pay, whereas the RP wants assurance so finds reason to pay.

The following uses are the most common for the application of an identity:

- Access control

- Authorizing an action (possibly through digitally signing) on a web site

- Providing proof of identity on an email

As the identity owner is the provider of information to the Identity Manager, it is normally beholden upon them to ensure that their identity information is current. While, contractually, the Identity Manager will normally insist on this, it is difficult for them to police. This may have some negative effect on the overall trust model; mechanisms need to be established where it is in the Identity Owner's interest to ensure information is kept up-to-date.

Within a PKI, the End Entity (EE) is the originator of an encrypted and/or signed communication. Identity is applied using either a private signing key, and optionally a private encryption key. In this environment, there is the requirement for the public key component of each key pair to be signed and formed into an X.509v3 digital certificate(s) by a CA. In the case of an encryption certificate, the EE will usually require this to be published in a publicly accessible area, such as an on-line directory.

The EE is the recipient of certificate management actions, which may take place automatically (e.g., key rollover) or at their direct request (e.g., key recovery).

If using encryption, the EE will need to conveniently source the public encryption certificate of the intended recipient.

**Relying Party**

The relying party is the recipient of an identity. As the relying party must trust the identity provided, there is a need to ensure that the level of trust is appropriate for the task in hand and that the identity is current.

For the former activity, the Relying Party will need to ascertain the policy against which the identity was issued by referring to the Identity Policy Authority. Assuming that the policies are not volatile, this action is only required once. However, it is helpful to the relying party if the policy used in issuing an identity is held with the identity so that checking can be minimized.

Thereafter the trust can be assumed as long as both the identity owner and the Identity Manager can also be trusted. Normally, trust in the Identity Manager can be assumed as long as they have the approval of the Identity Policy Authority; if not, the Identity Policy Authority is responsible for assuring that all identities issued by the Identity Manager are rescinded.

For each individual identity, a check of the current status must be made at the time it is required to be effective. Usually this requires a directory look-up against either currently valid IDs, or, more commonly, IDs that can no longer be trusted. While publishing these lists is normally undertaken by the Identity Issuer, it is the Identity Manager that holds the responsibility for ensuring the lists are accurate.

In PKI, the Relying Party is the recipient of an encrypted and/or signed communication, and thus may hold a private decryption key and/or check the signature of an End Entity embedded in a communication.

The Relying Party must decide whether to trust this certificate. This decision may to some extent be qualified by the assertions made in the Certificate Policy, issued by the RA, under which the certificate was issued. To this end, it is helpful if the certificate itself holds the policy.

The Relying Party may also need to consult a Certificate Revocation List to be assured that the certificate is still valid.

The Relying Party may configure access control system permissions or other certificate-using functionality based on these qualifications and/or assertions.

### Protective Hardware

As the use of electronic identity continues to grow in complexity and sophistication, the reliance on hardware devices to store identity credentials increases. Such devices range from single-purpose devices such as tokens and smart cards to sophisticated, general-use devices such as PDAs and tablet or notebook computers, with a variety of choices in between. Simultaneously, as the potential reach of any single digital identity increases, its value, and therefore the risk associated with its loss or theft, increases. As such, it is becoming increasingly important for the hardware itself to provide protection against tampering, eavesdropping, or other forms of malfeasance.

### Multi-OS Interoperability

Multi-OS interoperability for identity management does not require convergence toward a common authentication or authorization protocol. It does require convergence toward a common identity, such as UUID-pair. As a bit string, UUID-pair can be conveyed in any number of protocols and security assertion mechanisms such as SAML, either in native binary format or in an encoded form such as base64.

### Applications' use of the Operating System

For applications to consume identity credentials such as UUID-pair, two fundamental approaches are possible. The first approach is to provide a mechanism by which the application can communicate with the operating system. Such mechanisms include operating system interfaces such as GSS-API and directory query mechanisms such as LDAP. The second approach is to provide a mechanism by which two or more applications (e.g., a client and a server) can exchange credentials. SAML is emerging as a strong contender in this area.

### Data-Focused Protective Measures

A final area of concern for identity management is the provision of data-focused protective measures. By this it is meant that it is necessary to provide the ability to protect data independent of its deployment on any particular platform or its use by a particular application. As the use of XML becomes increasingly prevalent, the existence of data apart from platforms and applications will become increasingly common, and it will be necessary to provide protection in the form of integrity and privacy, and to preserve certain pieces of data as forensic evidence.

Mechanisms exist for providing the basic capabilities associated with these services, using a combination of symmetric and asymmetric encryption, time-stamping services, message digests, and digital signatures. What is missing is the association of any of these mechanisms with a common core identity. It is believed that the use of the common core identity mechanism described in this document, in conjunction with the existing cryptographic and time-stamping mechanisms, will be sufficient to provide the necessary protections.

### The Standards Bodies

This section surveys a number of standards bodies involved in various aspects of identity and permissions management.

#### Traditional International Organizations

**The ITU-T**: The International Telecommunications Union (ITU) is an organ of the United Nations (UN) within which governments and the private sector coordinate global telecommunications networks and services. Its Telecommunication Standardization Section (ITU-T) fulfils the purposes of the ITU relating to telecommunications standardization by studying technical, operating, and tariff questions and adopting Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The ITU-T was formerly known as the Committée Consultatif International Téléphonique et Télégraphique (CCITT). It started development of the X.500 series of recommendations for communication with and between directories.

**ISO/IEC**: The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from some 147 countries, one from each country. It is a non-governmental organization established in 1947, whose mission is to promote the development of standardization and related activities in the world. Its work results in international agreements that are published as International Standards.

Note that ISO is not a dyslexic acronym. It is a word, derived from the Greek *isos*, meaning *equal*, which is the root of the prefix in *isometric*, *isosceles*, etc.

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes international standards for all electrical, electronic, and related technologies. These serve as a basis for national standardization and as references when drafting international tenders and contracts.

Following an initial agreement in 1976, ISO and the IEC established their Joint Technical Committee No. 1 (JTC1) to develop standards for Information Technology, including standards for Open Systems Interconnection (OSI). These include the OSI standards for directory, whose

development was started by the ITU and continued in co-operation with ISO/IEC. They are published by the ITU as the X.500 series of recommendations, and by ISO/IEC as International Standard 9594.[10]

**National Bodies**

**ANSI**: The American National Standards Institute (ANSI) is the ISO member body for the USA. It is a private, non-profit organization that administers and coordinates the US voluntary standardization and conformity assessment system.

The Institute's mission is to enhance both the global competitiveness of US business and the US quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity.

**BSI**: The British Standards Institution (BSI) is the ISO member body for the United Kingdom. It is a UK corporation operating under a royal charter, but behaving in most respects as a commercial organization and known as the BSI Group. Its activities cover:

- Independent certification of management systems and products

- Commodity inspection

- Product testing

- Development of private, national, and international standards

- Management systems training

- Information on standards and international trade

British Standards is one of the BSI Group's businesses. It is the National Standards Body of the UK, responsible for facilitating, drafting, publishing, and marketing British Standards and other guidelines.

**INCITS**: The International Committee for Information Technology Standards (INCITS) is a US forum for information technology developers, producers, and users for the creation and maintenance of formal *de jure* IT standards. It is sponsored by the Information Technology Industry Council (ITI), a trade association representing the leading US providers of IT products and services. It is not an ISO member, but is accredited by, and operates under rules approved by, the US national standards body, ANSI.

The mission of INCITS is to produce market-driven, voluntary consensus standards in the areas of:

- Multimedia (MPEG/JPEG)

- Intercommunication among computing devices and information systems (including the Information Infrastructure, SCSI interfaces, and Geographic Information Systems)

- Storage media (hard drives, removable cartridges)

- Database (including SQL3)

- Security

---

[10] ISO/IEC 9594-1:1998, Information Technology – Open Systems Interconnection – The Directory.

• Programming languages (such as C++)

A complete list of ISO member bodies is available at
www.iso.ch/iso/en/aboutiso/isomembers/MemberCountryList.MemberCountryList.

**Professional and Trade Associations**

**IEEE**: The Institute of Electrical and Electronics Engineers, Inc. (commonly referred to as the IEEE, pronounced Eye-triple-E) is a non-profit, technical professional association with its headquarters in the USA.

The vision of the IEEE is to advance global prosperity by fostering technological innovation, enabling members' careers, and promoting community worldwide. Its mission is to promote the engineering process of creating, developing, integrating, sharing, and applying knowledge about electro and information technologies and sciences for the benefit of humanity and the profession.

The IEEE is an important standards-producing body. A number of the technical standards that it has produced have achieved worldwide acceptance.

**ABA**: The American Bar Association (ABA) is a voluntary professional association for lawyers. Its mission is to be the national representative of the legal profession for the USA, serving the public and the profession by promoting justice, professional excellence, and respect for the law. It provides law school accreditation, continuing legal education, information about the law, programs to assist lawyers and judges in their work, and initiatives to improve the legal system for the public.

**Industry Standards Development Organizations**

**The IETF**: The Internet Engineering Task Force (IETF) is the body that defines the standards that govern the Internet. It is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

The IETF is responsible for the Lightweight Directory Access Protocol (LDAP), which is the primary means by which directories are accessed over the Internet.

**W3C**: The World Wide Web Consortium (W3C) is the body that defines the standards that govern the web. (In protocol terms, the protocols defined by the W3C standards are layered on top of those defined by the IETF standards.) It was set up by the Laboratory for Computer Science at the Massachusetts Institute of Technology (MIT) in collaboration with the European Laboratory for Particle Physics (CERN), where the World Wide Web was invented. Its members include vendors of technology products and services, content providers, corporate users, research laboratories, standards bodies, and governments.

**OASIS**: The Organization for the Advancement of Structured Information Standards (OASIS) is a not-for-profit, global consortium that drives the development, convergence, and adoption of e-business standards. It was founded in 1993 under the name SGML Open as a consortium of vendors and users devoted to developing guidelines for interoperability among products that support the Standard Generalized Markup Language (SGML). It changed its name in 1998 to reflect an expanded scope of technical work, including the Extensible Markup Language (XML) and other related standards. Its activities include:

- **Directory Services**: This Technical Committee is developing DSML, an XML specification for marking up directory services information.

- **Access Control Markup Language (XACML)**: The purpose of the XACML Technical Committee is to define a core schema and corresponding namespace for the expression of authorization policies in XML against objects that are themselves identified in XML.

- **Provisioning Services**: The purpose of the OASIS Provisioning Services Technical Committee is to develop an end-to-end, open, XML-based framework specification for exchanging user, resource, and service provisioning information based on previous specifications such as ADPr, XRPM, ITML, and others.

- **XML-based Security Services**: This Technical Committee is working on the Security Assertions Mark-up Language (SAML), an XML-based security standard for exchanging authentication and authorization information.

**The Liberty Alliance**: The Liberty Alliance is a consortium of technology and consumer-facing organizations that was formed in September 2001 to establish an open standard for federated network identity. Its vision is one of a networked world in which individuals and businesses can more easily interact with one another while respecting the privacy and security of shared identity information. Its goal is to create specifications that incorporate, leverage, and support other industry standards, allowing members and organizations to build products and services that will interoperate and promote secure federated identity management.

The Alliance has:

- A Business and Marketing Expert Group, which works on use cases and business templates, and encourages adoption

- A Public Policy Expert Group, which holds external dialog with policymakers and gives internal advice on requirements and specifications

- A Technology Expert Group, which develops the architecture and specifications

The Alliance has produced three White Papers and is developing a comprehensive set of specifications for federated identity management. It holds interoperability testing events to assist implementers to develop products that meet the specifications.

The White Papers cover:

- Business Benefits of Federated Identity

- Liberty Alliance Identity Architecture

- Identity Systems and Liberty Specification, Version 1.1: Interoperability

The Architecture encompasses three specification modules:

- Federation Framework

- Identity Services Interfaces

- Identity Web Services Framework

These modules are intended to apply within a framework of supporting protocols and services including HTTP, SOAP, SAML, and WSDL.

To date, the Alliance has produced:

- Their Version 1.1 specifications, which address the Federation Framework

- Their Version 2 specifications, which address Identity Services

**DMTF**: The Distributed Management Task Force (DMTF) is the industry organization that is leading the development, adoption, and unification of management standards and initiatives for desktop, enterprise, and Internet environments.

The DMTF is responsible for the Directory Enabled Network (DEN) specification. DEN is designed to provide the building blocks for more intelligent networks by mapping users to network services, and mapping business criteria to the delivery or network services. This will enable applications and services to transparently leverage network infrastructure on behalf of the user, empower end-to-end services, and support distributed network-wide service creation, provisioning, and management. DEN specifies a Common Information Model (CIM) with LDAP mappings from CIM to the X.500 information model. This provides a template for exchanging information and enables vendors to share a common definition of a device, application, or service, and allows for extensions that add value.

### Consortia

There are a number of consortia working in areas related to identity management. Those of particular interest are described below.

**The Open Group**: The Open Group is a consortium of IT customers and vendors whose vision is Boundaryless Information Flow achieved through global interoperability in a secure, reliable, and timely manner.

The Open Group can produce specifications (it does not describe itself as a "standards body"). Its main activities in pursuit of its vision are:

- Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices

- Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies

- Offering a comprehensive set of services to enhance the operational efficiency of consortia

- Developing and operating the industry's premier certification service and encouraging procurement of certified products

The Open Group sees identity management as an important aspect of Boundaryless Information Flow. It has established an Identity Management Work Area, supported by four of its Forums (Directory Interoperability, Messaging, Mobile Management, and Security).

The Open Group Identity Management Work Area has produced an Identity Management Business Scenario. 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.

The Work Area is currently exploring:

- The options customers have for deploying identity management solutions using off-the-shelf products

- How the challenge of interoperability between different evolving identity management frameworks can be met

- Risk mitigation strategies for deploying identity management solutions

- Enterprise architectures for identity management, including a review and consideration of current practice

This document describes the considerations that The Open Group Identity Management Work Area will take into account and that will form its roadmap for producing deliverables.

**The WS-I Consortium**: The Web Services Interoperability Organization (WS-I) is an open industry effort chartered to promote web services interoperability across platforms, applications, and programming languages. It provides guidance, recommended practices, and supporting resources for developing interoperable web services. Membership is open to any organization supporting the goal of interoperable web services.

The WS-I is developing functional profiles of web services specifications. It has produced a basic profile and is working on usage scenarios and architectures for sample applications, and on a security profile.

The WS-I is also developing test tools to help implementers to achieve interoperability.

**The NAC**: The Network Applications Consortium (NAC) is a customer-oriented consortium that does requirements analysis and other work in the area of network applications. It has produced the Lightweight Internet Person Schema (LIPS) for directory representation of information about people. More recently, it has produced a position paper on Exploiting Directories in e-business Applications.

**International Initiatives**

**Trusted Transaction Roaming (T2R)**: This is a project whose purpose is to enable mobile subscribers to roam with wireless data services just as they do with voice services. Wireless digital identity management is one of its basic elements. It is sponsored by Radicchio, a European consortium whose aim is to establish a worldwide trust infrastructure and the accompanying business architectures for electronic transactions performed using wireless devices, such as mobile phones and PDAs.

**EURIM**: EURIM is a UK-based Parliament-Industry Group. Its mission is to provide Parliamentarians and other interested parties with clear, concise, accurate, balanced, and timely information on European IT-related Directives and policy proposals, to ensure that views and concerns are rapidly and effectively communicated to the Commission, Parliamentarians, and all other relevant organizations, and to ensure rapid, effective, and appropriate action should consensus become apparent. Its principal members are UK and European Parliamentarians. Its activities cover a wide range and include several topics related to identity management.

# Identity Management – The Legal Perspective

As the world grows smaller and more interconnected through IT, reliance on goodwill and social contracts needs additional support. Governments and other organizations all over the world have been enacting strong measures to protect personal information from unauthorized collection and disclosure. Following are some examples.

The European Union (EU) adopted a Data Protection Directive in 1998. This Directive has now been written into law in almost all EU member countries. Other EU Directives also address the issue of privacy. In the USA, sector-by-sector regulations have been adopted to protect the privacy of personal financial information (the Gramm-Leach-Bliley Act), personal medical information (the HIPAA Privacy Regulation), educational records (the FERPA Regulation), and personal information about minor children (the COPPA Act). Canada adopted a comprehensive national law (the PIPEDA Act) in 1998 to protect the privacy of personal information.

Legal requirements for privacy protection vary by locale. You will probably want to consult with your lawyers on privacy issues, in exactly the same way that you consult with them to shape your business practices for hiring and firing, labor relations, taxation, etc. But these are details. And simply meeting the law's minimum requirements is not the objective. The important point is that respect for privacy is important to you as a business person because it is important to the people who matter to your business: your customers, suppliers, and employees.

# Possible Next Steps

This section represents an action plan by which The Open Group can serve as a change agent for the industry.

## Architecture Guide

One possible next step is the development of an Identity Management Enterprise Architecture Guide. A starting point was produced in September 2003, and a decision was taken in principle to proceed with the development once the present White Paper is complete. If this decision is ratified in the light of the complete White Paper, then the Architecture Guide should be produced.

### The Starting Point

In September 2003, the Directory Interoperability Forum produced a paper on Identity Management in Enterprise Architecture for Boundaryless Information Flow. The paper was not published by The Open Group, but formed the basis for presentations that were given in the Plenary session of the October 2003 Open Group Conference, and in the associated Architecture Practitioners' Conference.

This paper is in two parts. The first part:

- Introduces the concepts of identity management and Boundaryless Information Flow

- Describes the role of identity management in the boundaryless enterprise

- Discusses the process of designing identity management into enterprise information systems

- Introduces a basic identity management implementation model

- Looks at the components that are available to build identity management solutions

- Considers the basic strategies for identity management implementation

The second part illustrates these ideas using three of six specific business models of Boundaryless Information Flow that were developed by The Open Group to provide focus for their Conference

### The Proposed Work

At its meeting during the Conference, The Open Group Identity Management Work Area agreed to expand the paper to develop an explanation that will benefit information systems architects of how to design identity management into enterprise IT infrastructure.

The Work Area agreed that:

- The title of the expanded paper should be "Enterprise Information Technology Architecture for Identity Management".

- The scope of this activity should include all aspects of identity management and its use in all kinds of enterprise.

- It should concentrate particularly on the role of identity management in Boundaryless Information Flow.

- It should be undertaken by the Identity Management Work Area, calling on the resources of its sponsoring forums and liaising with the Architecture Forum.

- Its intended audience should be information systems architects working in and for enterprises.

- The expanded paper should give them a better conceptual understanding of the role of identity management and how to design for it, plus specific practical recommendations and advice.

- The activity should result in a set of web pages on Designing Identity Management for the Enterprise.

- It could also be published in book form.

- A practical result will be to identify known approaches and characterize their usefulness for particular purposes.

It was agreed that the work should not commence until work on the present White Paper is substantially complete, to avoid dilution of resources. Now that the White Paper is substantially complete, work on the Guide can start, as agreed by the Work Area.

## Certification

One possible next step is the development of identity management certification programs. The Open Group is the industry's premier certification authority. It has already established two relevant certification programs: LDAP Certified and LDAP Ready. There are possibilities for developing further certification programs for identity management, and they should be considered.

One important factor that must be taken into account is that the Liberty Alliance, in conjunction with the IEEE, has started to define certification programs for identity management. The Open Group programs could be defined in cooperation with them, or in competition.

This section:

- Looks at what identity management certification might cover

- Compares the Liberty Alliance and The Open Group programs

- Identifies the possibilities for moving forward

### Identity Management Certification

Certification assures conformance to particular standards in the context of a model.

The Liberty Alliance has defined an identity management model and standards, and its program assures conformance to those standards. However, this model by no means embraces all of what the market today understands by identity management.

The Liberty Alliance model describes identity providers and consumers operating within circles of trust. Its standards are for protocols that support operations carried out by these providers and consumers, most notably single sign-on. There is an emerging body of products that implement these protocols and support these operations.

There are other identity management products, however, that support other operations. They include Access Control, Provisioning, Information Administration, Information Synchronization, Policy Management, Password Management, and Identity Information Storage (directory, meta-directory, and virtual directory).

There is an accepted model with standards for directory, and some standards in other areas (such as SPML for provisioning). The directory standards are from ISO/ITU and the IETF. These bodies have also produced standards for PKI, which is relevant to identity management. The other standards are largely from OASIS. There is also work in WS-I.

The Open Group has defined certification programs for directory. For certification programs to be created for other areas, models for those areas must be established, and new standards defined where necessary to fill gaps in existing ones.

## Comparison of Liberty Alliance and The Open Group Certification

The Open Group has defined two certification programs for directory: LDAP Certified and LDAP Ready. These programs are different in many ways, although they do share some common features.

### Legal Basis

They are all based on the granting of rights to use a trademark, and are governed by legal agreements that take the form of trademark license agreements.

For all three programs, the promises made about the products are made by their vendors, not by the certification authority.

### The Promise

For LDAP Certified and the Liberty Alliance program, the vendor promises that the product conforms to a specification. They are conformance certification programs. For LDAP Ready, the vendor promises that the product will interoperate with other products. It is an interoperability certification program.

### The Redress

For all three programs, the redress in case the promise is broken is withdrawal of the right to use the trademark. The effective sanction underlying this is high visibility in the marketplace that the product does not conform (or interoperate).

### The Evidence

The biggest difference between the three programs is in what evidence of conformance or interoperability is required before certification is granted.

- LDAP Certified has the strongest requirement. The product must pass a set of tests that have been defined by careful analysis of all the different cases covered by the specifications.

- The Liberty Alliance program has a less strong requirement. The product must demonstrate interoperability with other products at a Plugfest, and the protocol messages exchanged during that interoperation (which are captured by a sniffer) must be correct, but the interoperability cases covered are not based on rigorous examination of the specifications, and are relatively small in number.

- LDAP Ready has the weakest requirement. It has no minimum level of evidence, but it has guidelines for the strength of evidence that the vendor should provide, and it makes public the evidence provided so that whether the vendor meets the guidelines is visible.

**Third-Party Checking**

For LDAP Certified and the Liberty Alliance program, the certification authority checks the vendor's application, including the test results. In the case of the Liberty Alliance program, the checking is done almost in real-time at a Plugfest. This has the advantage of rapid turnaround, but the disadvantage that certification can only take place at Plugfests, which are at approximately six-monthly intervals. LDAP Ready operates on a self-certification basis, and there is no checking by the certification authority.

**Issues Arising During Certification**

Experience shows that issues often arise when a product is presented for certification as to whether details of product behavior are legal or acceptable. There can be gray areas in the specifications that are open to different interpretations. There can be minor product deviations that are strictly speaking illegal but are of low importance. LDAP Certified has clearly-defined procedures for resolving such issues. The Liberty Alliance program appears not to have such procedures. LDAP Ready does not have such procedures, but issues arise less frequently, because LDAP Ready is a self-certification program, and they can be "swept under the carpet" by the vendors.

**Post-Certification Issues**

Issues can also arise after certification. LDAP Certified and LDAP Ready have clearly-defined procedures for resolving such issues, which involve the vendor losing the right to use the trademark if the product is at fault. The Liberty Alliance program has provision for the vendor to lose the right to use the trademark, but does not appear to have clearly-defined procedures by which this can happen. This could leave the certification authority open to legal action by vendors.

## Possibilities for Moving Forward

There are three main are possibilities for moving forward. The Open Group can seek to cooperate with the Liberty Alliance, can seek to be independent of it, or can seek to compete with it.

### Co-operation

Cooperation with the Liberty Alliance might take the form of a marketing program that associates the Liberty Alliance program with LDAP Certified and LDAP Ready.

This should be backed by a revision of the programs to make them more similar. In particular, the LDAP Ready program should be strengthened by having some of the features of the

Liberty Alliance program incorporated in it. Also, the Liberty Alliance program would benefit by having the issue resolution features of The Open Group programs added to it.

Strengthening of the Liberty Alliance program by a rigorous analysis of the specifications to identify test cases, and the development of a formal test suite to test them, should be considered. This might be added to the program as an optional higher level of certification.

**Independence**

The Open Group could develop new certification programs in areas not covered by the Liberty Alliance, such as provisioning or information synchronization.

This would require the necessary models and standards to be defined and identified for those areas.

The certification programs would be similar to LDAP Certified in cases where conformance certification is appropriate.

In cases where interoperability certification is appropriate, programs similar to LDAP Ready might be defined, or stronger programs based on LDAP Ready but with added features from the Liberty program.

**Competition**

The Open Group could develop new programs as described above, but in areas that are already covered by the Liberty Alliance program. This course would be a departure from the normal Open Group policy, which is for collaboration with other consortia. It would only be justified if there were potent and highly visible reasons for it.

## Collaboration with the US Government on Guidelines for User Authentication

As already noted, the US Government, under the direction of the Office of Management and Budget (OMB), the National Institutes of Standards and Technology (NIST) is developing comprehensive guidelines for Identity Assurance that encompass:

- An Authentication Technical Model

- Registration and Identity Proofing

- Authentication Protocols

- Agency Process Requirements

These guidelines are being codified in Agency policy across the US Government civilian agencies.

As a potential "Next Step", it is proposed that The Open Group Identity Management Working Group works with the NIST policy developers to broaden the process to include private sector policy and/or standards recommendations. This effort will focus on furthering the interoperability of both government and industry solutions – based on interoperable standards.

NIST has invested considerable time and energy into developing the existing guidelines as basis for formal policy, and they are beginning to take considerable traction in the US Government. There can be both excellent "prior art" that could develop into standards as well

as lessons to be learned in the implementation of these guidelines that would be of great commercial benefit.

As "federation" of identities across organizations becomes more and more desirable, that federation will need to extend across government agencies as well as between commercial organizations. The Open Group, with both government and private sector membership could lead in the development of "federation" across government boundaries.

As a first step, The Open Group Identity Management Working Group could perform an analysis of the guidelines and resulting agency policies and practices and recommend adoption of appropriate elements of these for commercial adaptation and, if appropriate, standardization.

## Core Identity

There is a compelling need for a set of standards for specifying and exchanging a core identifier. Specifically, we are recommending the use of UUID-pairs for this purpose. At this time, we are aware of two industry standards under development that could assist in this purpose, and we propose that at least one additional standard is needed.

## UUID-Pair Attribute Type

We note that as part of its project to maximize the alignment between LDAP and X.500, the ITU-T and ISO/IEC collaborative committee on the directory is recommending that a new attribute type, known as UUID-pair, be added to the upcoming revision of X.520 (which is also to be published as IS 9594-6).

This specification is currently found in ISO/IEC JTC1 SC6 N12589, which is a Proposed Draft Amendment (PDAM) under ballot until March 5, 2004.

We support the inclusion of this attribute type and encourage members of The Open Group to do likewise.

## UUID Registration Procedures

We note that at its November 2003 meeting, ISO/IEC JTC1 SC6 produced a Committee Draft of IS 9834-8 (also identified as X.667) entitled "Procedures for the Operation of OSI Registration Authorities: Generation and Registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifiers". Conceptually, it appears that this registration procedure could be used in support of the "account authority" concept.

This Committee Draft is under CD ballot until March 5, 2004, and the stated intent is to progress it to Final CD following the resolution of any ballot comments. Although The Open Group has not developed a position on the content of this document, we encourage interested members of The Open Group to review the document for its suitability in support of the concepts we have set forward, and to follow their respective National Body procedures for producing comments on the document as deemed necessary.

## Source of Authority Discovery and Location

We have already discussed the need for the ability to automatically discover and locate registered UUIDs, and we suggested the possible use of DNS as the locator mechanism. It does

not appear that the UUID Registration document mentioned above addresses this concern. Therefore, as a possible next step, the Directory Interoperability Forum could review the issue and adopt a strategy for filling this gap.

## Standards Initiatives Co-operation and Integration

As awareness grows on the value of establishing a trustable identity across multiple environments, vendors and users have begun various initiatives to address this opportunity. These began as efforts in vertical industries. This has elevated to cross-industry efforts such as the Liberty Alliance, the WS-Security, and The Open Group Identity Management initiatives.

The trend toward coalescing these efforts is economic and strategically smart. However, given that the Liberty Alliance and the WS-Security efforts are based on different technical architectural approaches, the chances of resulting in a single specification are low.

A potential "Next Step" for The Open Group Identity Management Working Group (IDWG) could be to leverage its third-party perspective to facilitate an integrative approach amongst the standards to enable a cooperative trust between the systems. The key is to determine a trusted authentication hand-off mechanism. One approach may be to lead an effort which takes the NIST Authentication Technical Model as a reference point for negotiation. This would introduce a third-party language to the Liberty Alliance and WS-Security teams, thus minimizing proprietary aspects.

# Appendix A: Example Risk Assessment Methodology

## Assessing Risks

The identity management risk assessment has to be underwritten by sufficiently high management level. Where possible, it is recommended to have one identity management risk assessment for similar environments in the enterprise. This will improve overall security by setting a standard level and consistent implementation of security controls.

Identity management risk assessment is about the contribution the individual makes to the overall business risk. To arrive at the identity management risk:

3.  Conduct a business risk assessment.

4.  Determine the contribution of the individual to that risk.

5.  Identify the identity management controls that mitigate the risk.

There are three areas of business risks to be assessed:

• Risk to the organization: This can be measured in terms of harm to people, damage to image, or direct financial loss. Threats and vulnerabilities have to be identified and quantified in terms of likelihood and impact.

• Statutory, regulatory, and contractual requirements: These include requirements that the organization, its partners contractors, and service providers have to satisfy.

• Existing policies, objectives, and requirements: These include requirements for information processing that the organization has developed to support its operations.

The following table is only a guide and not exhaustive. Additional threats can be included when necessary. If any of the boxes under "Increased Likelihood" or "Increased Impact" is indicated for your application or information, you should seriously consider a more detailed risk assessment.

| Risks | Threats | Increased Likelihood | Increased Impact |
|---|---|---|---|
| To organization | Deliberate | | |
| | Eavesdropping | | |
| | Information Modification | | |
| | System Hacking | | |
| | Malicious Code | | |
| | Theft | | |
| | Accidental | | |
| | Errors and Omissions | | |
| | File Deletion | | |
| | Mis-routing | | |
| | Physical Accidents | | |
| To statutory, regulatory, and contractual | Breaches of the Criminal Law | | |
| | Breaches of US Export Controls on Data | | |

| Risks | Threats | Increased Likelihood | Increased Impact |
|---|---|---|---|
| contractual requirements | Breaches of National Data Protection Legislation | | |
| | Defamation | | |
| | Copyright Infringement | | |
| | Breaches of Contract | | |
| | Failure to Exercise Due Diligence on Safety Matters | | |
| To existing policies, objectives, and requirements for information processing | Breach of Business Principles | | |
| | Breach of Business Communication Principles | | |
| | Breach of Group Classification Guidelines | | |

Whether or not an organization mandates a detailed risk assessment methodology, a recognized method must be applied. It is recommended to use a standard that is used in your business for other assessments, as this will ensure consistency in your business. An example risk assessment matrix is shown below.

| Potential Consequences | | | | | | Increasing Probability | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | A | B | C | D | E |
| Rating | People | Financial Loss | Environment | Reputation | Quality of Services & Products | Never heard of in the industry | Heard of in the industry | Has occurred in the industry | Happens several times per year in industry | Happens several times per year in the industry |
| 0 | No injury | No loss | No impact | No impact | No complaints | | | | | |
| 1 | Slight injury | <$100.000 | Slight impact | Slight impact | Off spec/not delivering | | | | | Serious risk (5) |
| 2 | Minor injury | <$500.000 | Minor impact | Limited impact | Formal complaint (external) | | | Serious risk (6) | Serious risk (8) | High risk |
| 3 | Major injury | <$3 million | Localized impact | Considerable impact | Complaints of several customers | Serious risk (3) | Serious risk (6) | Serious risk (9) | High risk | Intolerable risk |
| 4 | Single fatality | <$10 million | Major impact | Major national | Loss of customers | Serious risk (4) | Serious risk (8) | High risk | Intolerable risk | Intolerable risk |
| 5 | Multiple fatalities | >$10 million | Massive impact | Major international | Considerable loss of market share | Serious risk (5) | High risk | Intolerable .risk | Intolerable risk | Intolerable risk |

Explanations of ratings for the categories that are not entirely self-explanatory follow:

| Rating | People |
|---|---|
| 0 | **No injury or damage to health.** |
| 1 | **Slight injury or health effects** (including first aid case and medical treatment case). Not affecting work performance or causing disability. |
| 2 | **Minor injury or health effects** (lost time Injury). Affecting work performance, such as restriction to activities (Restricted Work Case) or a need to take a few days to fully recover (Lost Workday Case). Limited health effects that are reversible; e.g., skin irritation, food poisoning. |
| 3 | **Major injury or health effects** (including Permanent Partial Disability). Affecting work performance in the longer term, such as a prolonged absence from work. Irreversible health damage without loss of life; e.g., noise-induced hearing loss, chronic back injuries. |
| 4 | **Single fatality or permanent total disability**. From an accident or occupational illness (poisoning, cancer). |
| 5 | **Multiple fatalities**. From an accident or occupational illness (poisoning, cancer). |

| Rating | Environment |
|---|---|
| 0 | **No impact**. No environmental damage. |
| 1 | **Slight impact**. Local environmental damage. Within a confined area and within systems. Negligible financial consequences. |
| 2 | **Minor impact.** Contamination. Damage sufficiently large to attack the environment. Single instance of exceeding statutory or prescribed criterion. Single complaint. No permanent effect on the environment. |
| 3 | **Localized impact**. Limited loss of discharges of known toxicity. Repeated instances of exceeding statutory or prescribed limit. Affecting neighborhood. |
| 4 | **Major impact**. Severe environmental damage. The company is required to take extensive measures to restore the contaminated environment to its original state. Extended instances of exceeding statutory or prescribed limits. |
| 5 | **Massive impact**. Persistent severe environmental damage or severe nuisance extending over a large area. In terms of commercial or recreational use or nature conservancy, a major economic loss for the company. Constant, high instances of exceeding statutory or prescribed limits. |

| Rating | Reputation |
|---|---|
| 0 | **No impact**. No public awareness. |
| 1 | **Slight impact**. Public awareness may exist, but there is no public concern. |
| 2 | **Limited impact.** Some local public concern. Some local media and/or local political attention with potentially adverse aspects for company operations. |
| 3 | **Considerable impact**. Regional public concern. Extensive adverse attention in local media. Slight national media and/or local/regional political attention. Adverse stance of local government and/or action groups. |
| 4 | **National impact**. National public concern. Extensive adverse attention in the national media. Regional/national policies with potentially restrictive measures and/or impact on grant of licenses. Mobilization of action groups. |
| 5 | **International impact**. International public attention. Extensive adverse attention in international media. National/international policies with potentially severe impact on access to new areas, grants of licenses, and/or tax legislation. |

# Appendix B: Additional Business Scenarios for Identity and Access Management

*Note that copyright for the material in this Appendix is held by The Securities Industry Middleware Council, Inc. Permission to reprint has been granted, subject to the conditions specified in the front matter of this document.*

These scenarios are not "identity management scenarios". These are representative business scenarios of the securities industry that a useful identity management infrastructure or technology would be used to support. An identity management solution that would be widely acceptable and durable in the securities industry must be able to address (or be used in) all of these scenarios. A solution that finds some of these scenarios intractable would be of little use, no matter how well it supported the remaining scenarios.

In the next phase of the initiative, these scenarios will be worked out in more detail, including a more comprehensive description of the "constraints" under which they must work. (We will treat trust and accountability requirements and compliance obligations as constraints rather than requirements.)

### Trust Scenarios

**Identity-Based Trust: Basic**

**SYNOPSIS**

In this scenario, a service provider relies on a third-party Identity Authority to allow reliable identification of a party requesting service. While the Identity Authority may provide guarantees about his own work in uniquely and unambiguously identifying the requestor, he does not provide any assurance about the requestor's likely behavior in fulfilling obligations to a transaction.
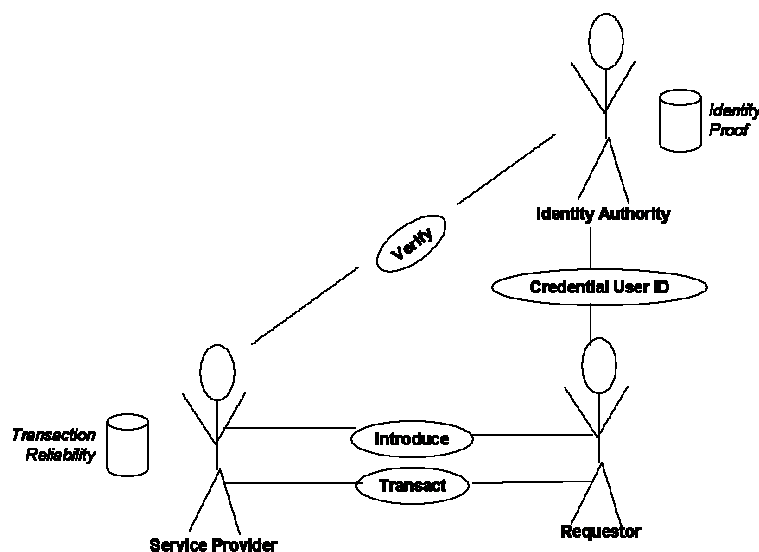


**STEPS**

1.  Identity Authority credentials the requestor's identity. This may involve vetting the requestor to determine that his claimed identity is valid.

2.  The requestor introduces himself to the service provider, demonstrating his identity with the credential issues by the Identity Authority. The service provider performs whatever checks and enrollment processes his policy requires to allow him to authorize subsequent transactions.

3.  At any time, the service provider may verify the continued validity of the requestor's identity credential with the Identity Authority.

4.  Requestor transacts business with the service provider by demonstrating that his is the identity by which he introduced himself to the service provider. Based on the nature or outcome of the transaction, the service provider may update his information about the requestor's reliability in business transactions for use in subsequent authorization (risk assumption) decisions.

**NOTES**

- The "Introduce" step may be equivalent to the Account Provisioning scenario.

- The Identity Authority may qualify the level of assurance of identity he provides. He may also constrain the contexts in which his assurances will be valid. The Identity Authority might also provide, as part of the identity qualifiers, information such as the organizational affiliation of the requestor. (This makes the credential less flexible as an identity token, possibly requiring the issuance of different identities to the same principal if he has roles in multiple organizations, or even multiple roles in a single organization.) The service provider might infer from any of these constraints or qualifications that the requestor is more or less trustworthy for particular sorts or values of transaction.

- This scenario does not address the manner in which the requestor demonstrates that he has legitimate control of the identity credential issued by the Identity Authority. The Identity Authority may use techniques that ensure that only the requestor can have use of the credential. Alternatively, an additional authentication authority may be required to assure that the credential is actually being used by the requestor.

**Role-Qualified Identity-Based Trust**

**SYNOPSIS**

In this scenario, a service provider relies on a third-party Identity Authority to allow reliable identification of a party requesting service and on a Role or Privilege Authority to provide information about the sort of actions the requestor is entitled to undertake. While the Identity Authority may provide guarantees about his own work in uniquely and unambiguously identifying the requestor, he does not provide any assurance about the requestor's likely behavior in fulfilling obligations to a transaction. The sort of guarantees the Role or Privilege Authority might give for transactions entered into by the requestor in his assigned role or with his given privileges will depend on the contractual relation between the service provider and the Role or Privilege Authority.
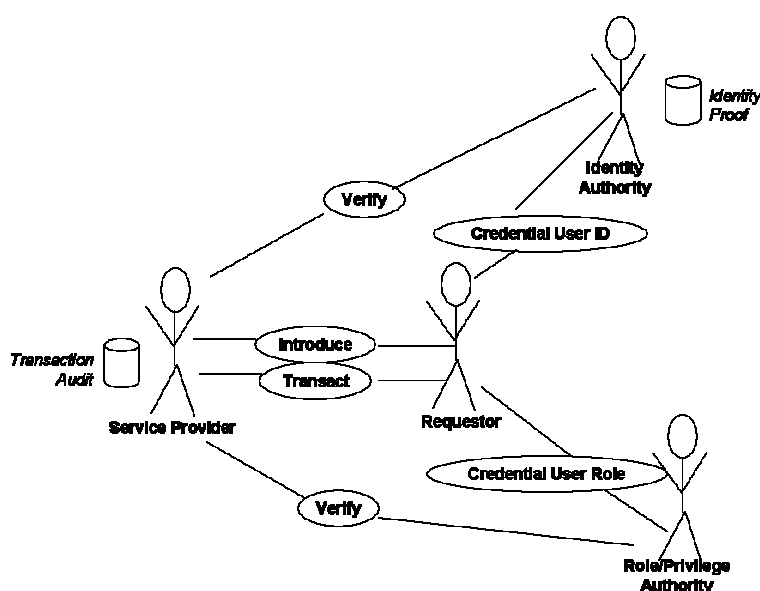


**STEPS**

1. Identity Authority credentials the requestor's identity. This may involve vetting the requestor to determine that his claimed identity is valid.

2. Role or Privilege Authority credentials the requestor's role. A binding is established between the role and identity credentials, so that poof of identity to a relying party may be used as the basis on which the use of the role or privilege credentials is to be trusted.

   The Credential User ID and Credential User Role processes may be combined into a single process performed by a single authority. In this case one vetting process is used for all credentialing. A single credential for identity and role may be issued, or separate but bound credentials may be issued for identity and one or more roles or privileges.

   Alternatively, the Role or Privilege Authority may operate as a service provider following the identity trust scenario.

3. The service provider may require requestors to introduce themselves prior to performing transactions. This requirement may be in support of trust/risk management policies, audit

or accountability policies, or operational or administrative constraints to transaction time account creation. At introduction, the service provider may determine whether to rely in whole or part on the implied guarantees of the role or privilege credentials.

4. At any time, the service provider may verify the continued validity of the requestor's identity credential with the Identity Authority, or role or privilege credential with the Role or Privilege Authority.

5. Requestor transacts business with the service provider by demonstrating that his is the identity by which he introduced himself to the service provider, and that the identity is bound to or associated with the Role or Privilege credentials that are simultaneously presented. The service provider records information about the transaction in association with the identity for purposes of audit, accountability, and/or regulatory compliance. Based on the nature or outcome of the transaction, the service provider may update his information about the requestor's reliability in business transactions for use in subsequent authorization (risk assumption) decisions.

**NOTES**

- See notes on the Identity Trust Scenario.

- When the role or privilege credentials are self-authenticating without reference to the requestor's identity, this scenario becomes a capability-based trust scenario.

- A requestor may obtain independent sets of role or privilege credentials from multiple Role or Privilege Authorities. In that case, it would be possible for different organizations or organization units to independently grant privileges or roles to a single person. How such privileges may be aggregated for evaluation by the service provider or other relying party would be a matter of policy for both the service provider and the Role or Privilege Authority.

**Transaction Authorized**

**SYNOPSIS**

In this scenario, a service provider relies on a third-party Identity Authority to allow reliable identification of a party requesting service and on a Role or Privilege Authority to provide information about the sort of actions the requestor is entitled to undertake. In addition, the service provider relies on authorizations of specific transactions undertaken by the requestor. These authorizations are provided by an entity with which the service provider has a contractual trust relationship, usually but not always the firm of which the requestor is an employee or agent. The authorizations are credentialed; that is, the requestor receives a verifiable credential attesting to his authority to enter into the transaction.
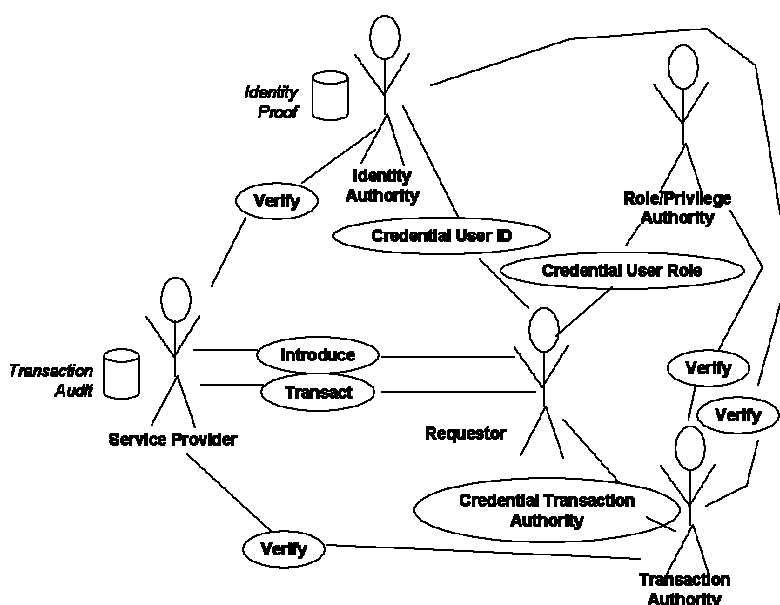


**STEPS**

1. Requestor credentials his authority, role, privileges, etc. by interacting with various authorities.

2. If required by the service provider, the requestor introduces himself to the service provider.

   In this scenario the introduction is based on the requestor's identity. In variant scenarios, the service provider might accept introductions (enrollments) of groups, and individual requestors would relate themselves to those introductions by presenting role credentials attesting to group membership.

3. Requester obtains credential attesting to his authority to initiate a specific transaction. The "text" of the transaction along with the requestor's various credentials are provided to the transaction authority, which returns an authorization credential bound to the transaction and to the requestor's credentials.

   The authority credential may be bivalent (yes/no) or continuously valued (Dollar limit). In

the latter case, it signifies that the transaction may be authorized if its value does not exceed the limit.

Authorization credentials may have expiration values, and usage constraints.

4.  The requestor provides the service provider with his service request and all associated and supporting credentials.

**Prior Trust Establishment: Create (Client) Account**

**SYNOPSIS**

In this scenario, a service provider creates an account for a new client based on his identity, possibly with some additional information to support the claim of identity or his capability to open the account. In this scenario, there are no available guarantors of the requestor's ability to fulfill any obligations of the account, or to guarantee any transactions that may be done through or in the account.
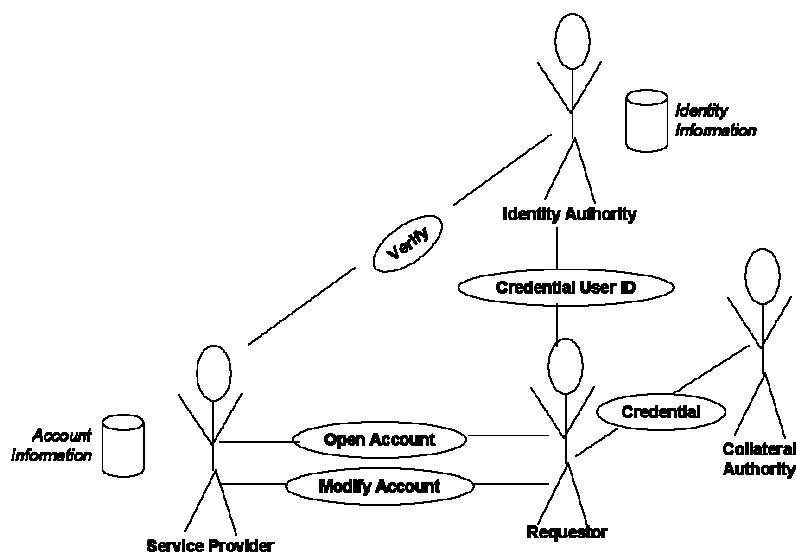


**STEPS**

1. Identity Authority credentials the requestor's identity. This may involve vetting the requestor to determine that his claimed identity is valid.

2. The requestor may obtain (or have) additional credentials supporting his request to create an account.

3. The requestor opens an account, presenting the identity and collateral credentials in support of his request. The service provider evaluates those credentials, and performs any other verifications and evaluations required by his policy. (Requesting a third-party credit check, for example, or searching his own records for previous experience with the requestor.) The service provider may grant or deny the request to open an account.

   This may be a synchronous or asynchronous operation. That is, the service provider may provide the results of the request as an immediate response to the request, or it may complete the request, and indicate that the final results will be returned at a later time, possibly through a different channel.

4. The service provider may provide the requestor with a privilege or attribute credential to allow him subsequent access to the account.

   Alternatively, the service provider may rely on the third-party identity credential to associate subsequent requests with the proper account.

5.  Subject to privacy, fair credit, and other similar regulations, and to the contract between the service provider and the requestor, the service provider may at any time during or after the opening of the account verify the continued validity of the requestor's identity and collateral credentials with the issuing authorities.

6.  Requestor may subsequently modify aspects of his account (including closing the account).

**NOTES**

•   See also the Identity-based Trust Scenario.

**Client Referral**

**SYNOPSIS**

In this scenario, a referring service provider with whom the requestor has a relationship (requestor is a client of the referring service provider) requests another service provider to create a subsidiary or related account for the client. The second service provider may provide services that are subsidiary to the services provided by the referring service provider, or they may be complementary. The second service provider's service may be "white labeled", appearing to the requestor to be services of the referring service provider. In many cases, accountability, audit, and supervisory obligations will require some amount of sharing of information on account activity and status between the referring service provider and the second service provider.
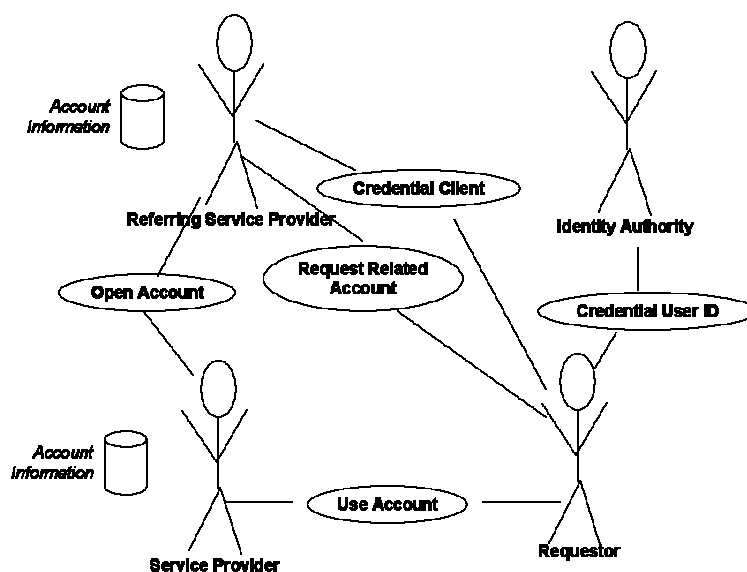


**STEPS**

1. The requestor has previously created an account with the referring service provider. He will have acquired some set of credentials from the referring service provider and/or third-party credentialing services that allow the requestor to access this account.

2. Requestor requests referring service provider to create an account for requestor at a second service provider.

   The request may be implicit rather than explicit. For example, the client may request a service that is in whole or part outsourced by the referring service provider, and requires the creation of an account with the second service provider. Whether the client is (or even is allowed to be) aware of the existence of the account at the second service provider may affect the choice of mechanisms used to accomplish this scenario.

3. The referring service provider communicates the request to the second service provider, including any necessary information describing the client. This may include information describing the credentials the client is known or supposed to have, information about the client received by the referring service provider from independent sources, and

information about the client and his account developed by the referring service provider.

**NOTES**

- This is not identical to single sign-on. The two service providers may use unrelated session establishment methods.

- There is no requirement that the Requester be in a session with either service provider to use the services of the other.

- The second service provider may offer services similar to those of the referring service provider, but in a different medium; e.g., wireless services. This may affect implementation options.

### Access Scenarios

**Parallel Access**

**SYNOPSIS**

A trader for a firm is given, by the firm, privileges to trade on the firm's behalf. These credentials are to be presented to the trading platform (market center, exchange, or other trading venue) both to claim the authority to trade, and to identify the firm as the counter-party (or guarantor) of the trade.

The trader may place trade orders through more than one channel, including interactive services (perhaps implemented as web services) and asynchronous services (perhaps implemented with older protocols such as FCS or FIX, or with newer protocols based on XML).

Trade orders should be treated identically by the policy enforcement mechanisms of the trading platform regardless of the channel through which they are placed. The resulting trades must be identically attributed for audit and other accountability purposes.
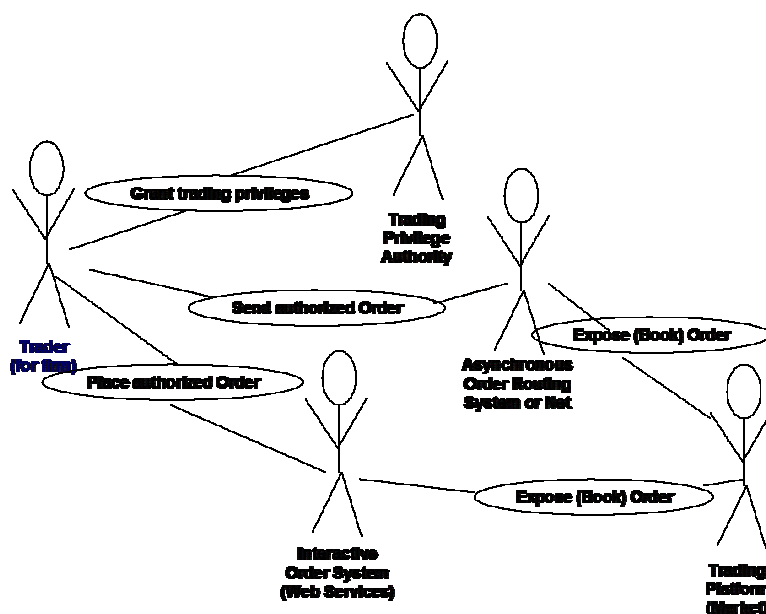


**STEPS**

1. The Firm's Trading Privilege Authority grants trading privileges to the trader.

2. Trader sends an order to an asynchronous order system or net (e.g., SuperDOT™).

3. The order system exposes the order to the trading system (or market).

4. Trader interacts with interactive order system which functions as a "portal" to the trading platform.

5. Orders created in the interactive system are exposed to the trading platform.

**Acknowledged Access**

**SYNOPSIS**

In this scenario, a trader at a firm is given trading privileges by the firm. The trader presents the privileges to an Exchange system when he enters an order. The Exchange system consults an Exchange Authorization Policy system, which acknowledges the privileges granted by the firm. The fact that the Exchange has acknowledged the privileges enhances their credibility to downstream processors such as clearing and depository companies. As important, the Exchange has accepted the order, which may be executed and require the trader to follow its post-trade processing at the depository. The fact that the Exchange has acknowledged the privilege should be sufficient to induce the downstream processor to grant access.
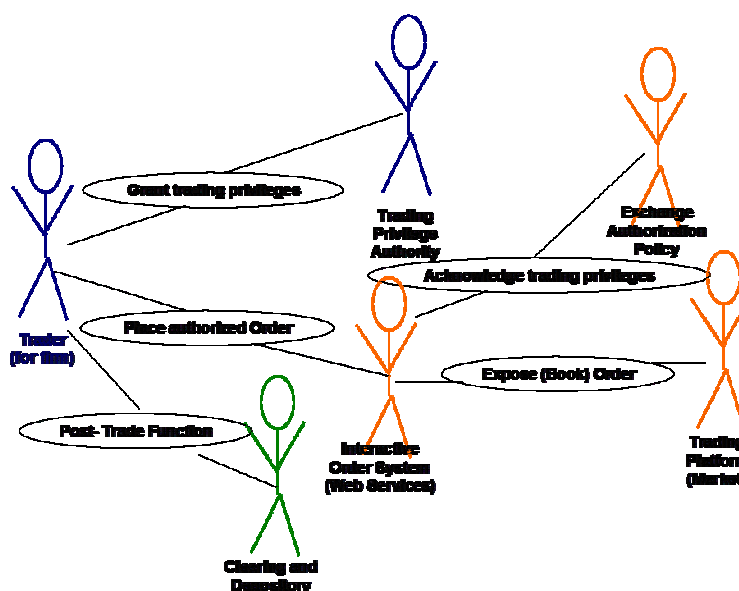


**STEPS**

1. The Trader obtains his credentials by authenticating himself to his firm's systems, and by meeting any other policy requirements.

2. The Trader uses the credentials to place an order on the Exchange's interactive order placement system. (May be a web services model.) (Steps 3 and 4 are performed before this step completes.)

3. The Exchange's interactive order system consults the exchange's authorization policy system that returns an assertion concerning the trader's authorization to place the order (or any orders) on the exchange.

4. The interactive order system exposes (forwards) the order to the trading system and returns an acknowledgement to the trader. The order acknowledgement may include the assertion by which the Exchange Authorization Policy system acknowledged the firm's grant of trading privileges to the trader, enhancing or extending the Trader's credentials.

5. The Trader presents his enriched credentials to subsequent processing steps, including, for example, clearing and depository systems.

## Trading and Order Handling Scenarios

### Order Routing (e.g., FIX) Network

**SYNOPSIS**

In this scenario, a buy-side firm enters an order by way of a FIX network. (In this scenario, the network operator is not a financial guarantor of the order.) It is delivered to one of several sell-side firms. Choice of the sell-side firm may be made by the originating buy-side firm, or may be delegated to the routing network on some basis. ("Order" is representative of any of a number of functions that are represented in conventional order management protocols.) The order is delivered to the sell-side firm and is identified as being – for the purposes of authority and accountability – from the originating buy-side firm.

Whether the order routing network is explicitly identified as an intermediary in the delivery of the order may depend on such things as the amount of discretion the network was given in routing the order.

The same operation – Enter Order – is shown at all points, between the buy-side firm and the network, and between the network and the sell-side firm. Sell-side recipients of orders do not provide different services to directly connected clients than they provide to clients connected through a network. Similarly, the systems of the buy-side firm ought not need to implement different functions for sending orders through networks than they do for other means of delivery.
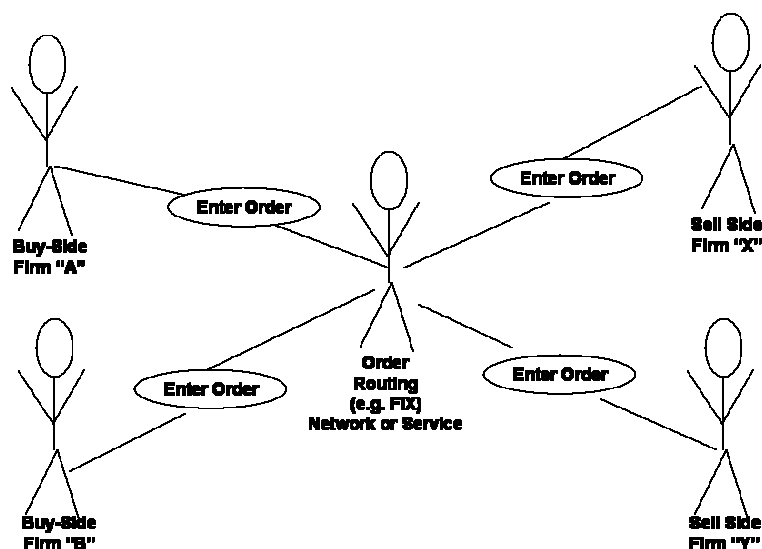


**STEPS**

1. The buy-side firm enters an order by sending an order message including an identity credential. The identity credential may be explicitly included in the message, or implicitly associated with the message by means of a session security function.

2. The order routing network makes a routing decision which may be based on one or more of the following criteria:

3. Explicit routing instructions from the buy-side firm

4. The privileges of the buy-side to transact business with any of the sell-side firms

5. Prices or other terms offered or exposed by the sell-side firms

6. Other preferences that may be expressed by the buy-side firm

7. If required[11], the Order Routing Network adds its identity as an intermediary to the identity of the buy-side firm as principal.

8. The Order Routing Network enters the order to the sell-side firm.

---

[11] The explicit identification of the order routing network as an intermediary may be required by one or more sell-side firms, by exchanges of which the sell-side firms are members, by other industry self-regulatory organizations, by accounting or audit regulations, etc.

**Anonymous Order Placement**

**SYNOPSIS**

In this scenario, a Trader for an institution enters orders directly to an exchange or other market center without the order being seen by any intermediary. The "anonymity" provided in this scenario is not absolute anonymity, since the Exchange will "know" the identity of the institution placing the trade. This anonymity might better be called privacy with respect to brokers and other intermediaries.

The form of privacy or anonymity provided by this scenario may be combined with other privacy or anonymity scenarios to provide more complete privacy, pseudonimity, or anonymity.

The goal of this scenario is to allow the institutional trader to place orders without the prior or concurrent knowledge of the broker or guarantor, while still allowing the broker or guarantor to exercise the supervision required by regulation and by his need to monitor the risk he assumes by providing credit guarantees to the institution.

This version of the scenario shows the credit backing being given by the brokerage to the institution, then subdivided by the institution for use by individual traders. As the Trader places orders that rely on the backing, the Exchange (or other relying party) indicates to the institution the amount of backing that was actually consumed by the order.

Not shown in this basic scenario is the means by which the Supervisory Authority is advised of the activity that relies on his guarantees, or the mechanism by which the decrease in remaining credit is correctly reflected in the credentials of the individual trader.

This scenario may not in fact be implementable. Alternate scenarios showing various ways these objectives may be achieved will be derived from this basic scenario.
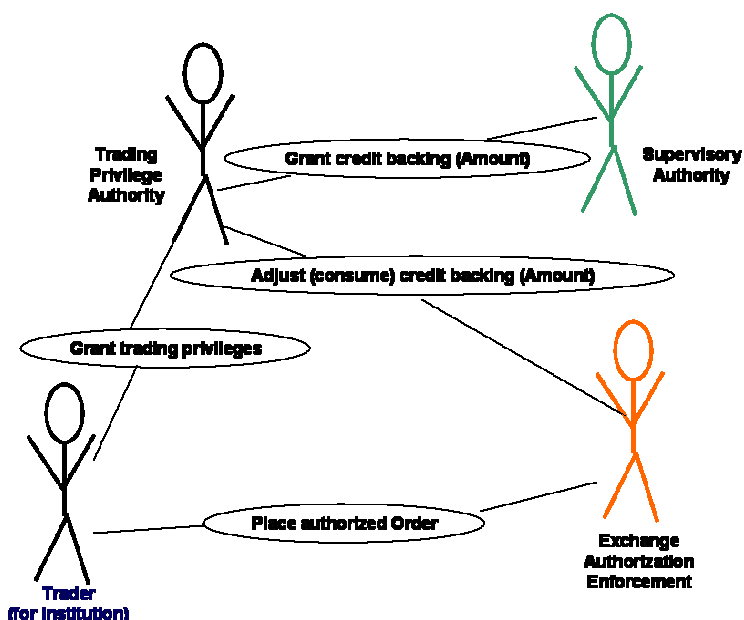
**STEPS**

1. The supervisory authority (typically a brokerage or sell-side firm) provides the institution with credit backing (guarantees) of a certain amount. That backing is provided to the institution's Trading Privilege Authority.

2. The Trader for the institution is granted trading privileges by the institution's Trading Privilege Authority. These may include:

3. Assertions about the Trader's identity and the quality of its authentication

4. The sort of transactions the trader may undertake

5. The counter-parties to which he is accredited

6. The portion of the firm's credit backing he is entitled to rely on in his trading activities

7. The Trader places an order with the Exchange.

8. The Exchange advises the institution how much of the guarantee was required to back the order.

   Since it is the exchange that relies on the guarantee, and also the exchange's market that sets the price at which the order will execute, the exchange determines the exact amount of credit backing required to support the order.

**Broker-to-Broker Trade**

**SYNOPSIS**

This scenario is based on "Following a Trade", a scenario described in the Depository Trust & Clearing Corporation (DTCC) web site (http://www.dtcc.com/).

In this scenario, a transaction initiated by matching buy and sell orders placed by individual investors is executed, cleared, and settled. Note that this transaction is a multi-day transaction. There may be an arbitrary delay between steps 1 and 2. Step two defines Trade Day (T). Subsequent days are called T+1, T+2, and so on.
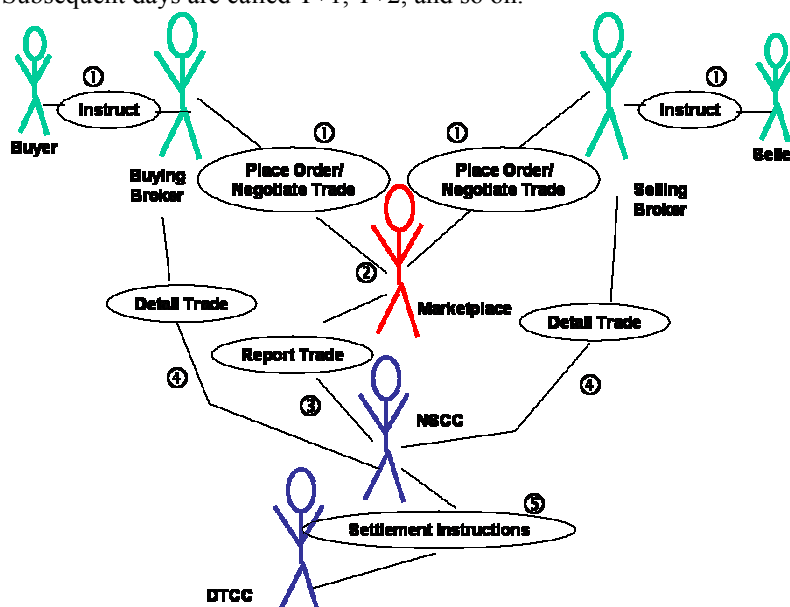


**STEPS**

1. The trade begins when a buyer or seller sends an order to a broker-dealer to execute a trade. The broker-dealer routes the order to a marketplace (NYSE, NASDAQ, Amex, or regional exchanges) or other trading mechanisms (ECNs) for execution. The trade is arranged with another broker-dealer or specialist.

2. Trade Date (T): Once the trade details are agreed, the information is sent, usually by the marketplaces, to NSCC for post-trade processing. With advances in technology, most equity transactions are now sent as "locked-in" trades, which means that the marketplace has already compared (confirmed all details) the trades being reported to NSCC. Others are sent in directly by broker-dealers. With most bond trades (and some stock trades), each broker-dealer submits its side of the trade to NSCC, and NSCC compares both sides to see that all details match.

3. T+1: On T+1, NSCC issues to participating firms computerized reports known as "T contracts". These contracts, the legally binding documents for a trade, show the details of all locked-in trades. These documents confirm that the transactions have compared and are ready for settlement in the Continuous Net Settlement (CNS) system. NSCC's guarantee of settlement begins after midnight of T+1 when it reports back to its customers that the trades have been compared.

It is at this point that NSCC assumes responsibility for settling the transaction (even if a member firm goes out of business). Transactions that fail to match are reported back for corrections.

4. T+2: On T+2, NSCC issues to broker-dealers a summary of all compared trades, the net positions, and the money settlement that will be required the following day, which is settlement day.

5. T+3: On settlement day (T+3), NSCC also nets the dollar amounts that broker-dealers will receive from or pay to NSCC to satisfy their trading obligations for the day. NSCC then issues money settlement instructions to each broker-dealer and its settling bank. Each broker-dealer member of NSCC is required to designate a bank that will handle money settlement for the trades. Based on these instructions, NSCC either wires the bank money, or has the bank wire NSCC money to settle the broker-dealer's obligations. NSCC and the banks use the Federal Reserve electronic wire (or Fed Wire) system to electronically transfer funds the same day. Since all money obligations are netted, a single wire transfer can settle all the obligations for all securities handled by a broker-dealer through NSCC for an entire trading day. NSCC also maintains an account at DTC through which it can issue instructions for book-entry transfer of securities to or from customers' accounts, depending on whether they owe or are owed these securities.

**Custodial Trade Processing**

**SYNOPSIS**

This scenario is based on "What is Straight Through Processing: The Custodian's View", a presentation by Kevin R. Smith, Senior Vice President of The Bank of New York, given at SIMC's November 16, 1999 general meeting.

In this scenario, a transaction initiated by an investment manager is "allocated" to the custodial accounts of an arbitrary number of clients.

Identity is relevant in several forms:

• Verifying the authority of each actor to perform the actions appropriate to his role in the transaction

• Accounting to each concerned party (including regulatory actors not shown in the diagram) for the responsibility, liability, and other regulatory compliance of the original and subsequent parties to the transaction

• Identifying the principals (accounts) to/from which the proceeds of the transaction should be credited/debited. (This may not be known at the time the transaction is initiated.)
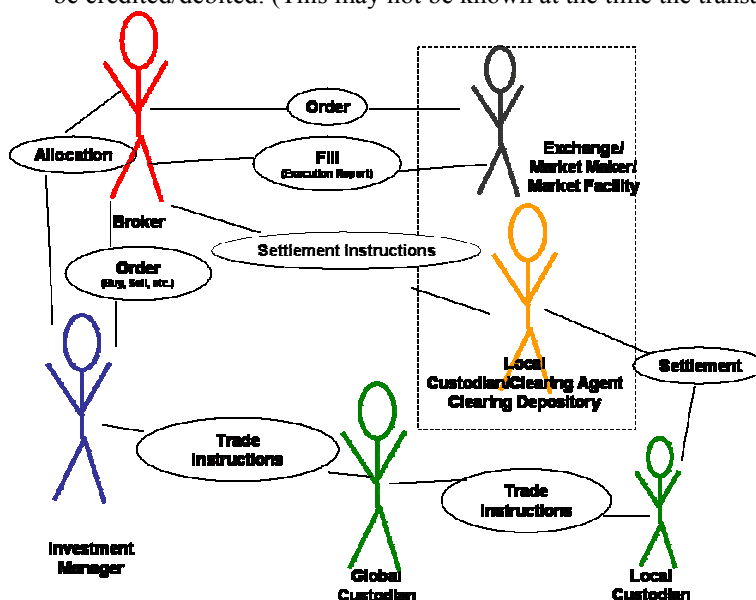


**STEPS**

1. The investment manager initiates an order to the broker to buy or sell securities. The investment manager may not yet know the basis on which any resulting transaction will be allocated among his clients.

2. The broker places the order with an exchange or other market facility.

3. The order is filled (and confirmed).

4. The broker and investment manager exchange information about the trade and its allocation.

5.  The broker and the clearing agent exchange information and instructions concerning settlement.

6.  The investment manager instructs the custodian on the settlement and allocation of the trade. This step may be subdivided by the global custodian to one or more local custodians. (This step includes the ultimate report by the custodian concerning the completion of the settlement.)

7.  The transaction is settled with the (local) custodian on behalf of the clients of the Investment Manager.

**Access Intermediaries: Trading Hub**

**SYNOPSIS**

The hub serves as a central point of communication between and among participant firms, allowing them to post (advertise) their inventory of securities (offers) or their desire to acquire securities (bids). (Bids and offers are collectively called interest.) The hub is not a pass-through; firms may choose to have their interests posted anonymously.
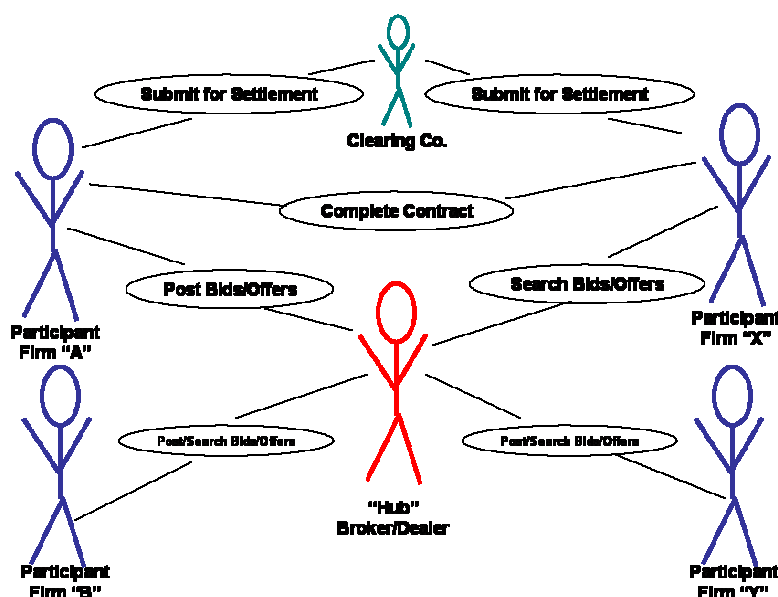


In this scenario, the participants are peers to each other, and have prearranged trust among themselves. With regard to the rules of the hub's market, the trust is mediated by the hub. With regard to settlement of the transactions, this trust is mediated by a clearing company.

The hub is a broker/dealer allowing it to intervene in the process by which bids and offers are aggregated, displayed, matched, and allocated to counter-parties. This provides the participating firms with additional opportunities to achieve "market anonymity".

**STEPS**

1. Participating firms post bids and offers at the hub. The hub may display the interest in aggregate or as individual bids/offers. The hub may identify matching bids and offers.

2. Participating firms search the postings at the hub for bids or offers they may want to take. (If the hub identifies matches, it is essentially performing this step on behalf of participants who have posted interest.)

3. Identified opportunities for bids and offers to match are selected for execution by a process that may be performed or assisted by the hub. (This may involve establishing priorities and precedence or allocations for competing interest.)

4. Participants whose interests are selected for execution complete contracts for the transaction. The form and manner of completion of these contracts may be specified and/or assisted by the hub.

5.  Participants submit their contracts to the clearing company[12], identifying the counter-party, for comparison, clearance, and settlement. The hub may facilitate this reporting, or it may submit its own reports to aid in comparison of the contacts submitted by participants.

---

[12] BondHub was used as the model for this scenario. BondHub operates under the supervision of the MSRB. MSRB Rule G-14 requires dealers to report inter-dealer transactions to the MSRB through the Fixed Income Transaction System operated by the National Securities Clearing Corporation (NSCC). The procedures for reporting inter-dealer transactions require that dealers identify themselves and the contra-parties with which they are effecting transactions.

**Trading Portal**

**SYNOPSIS**

A "portal" serves as a consolidator of and single point of access to services for a number clients. The portal may be a separate business entity, or it may be a facility of a service provider. Portals that are operated by consortia of service clients or service providers would be considered separate businesses from the members of the sponsoring consortium. Consortium or community of interest portals may be a special case for identity or privilege management, because they can form special trust relationships with their sponsors.
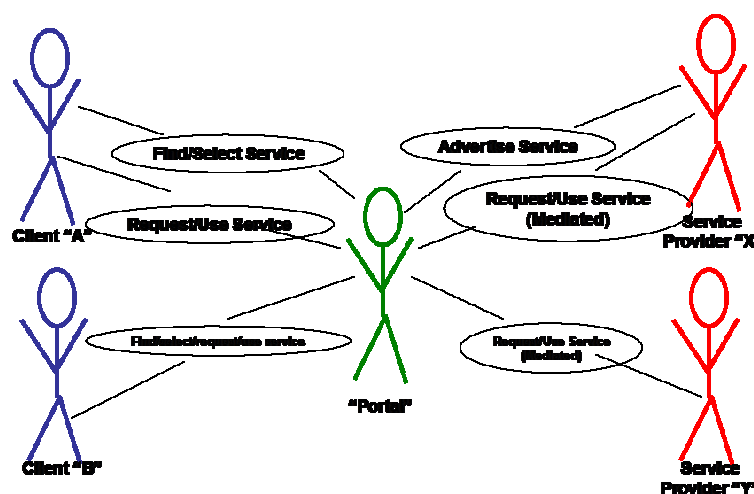


**PARTIES**

In this scenario, the participants are not peers. Service clients and service providers have distinct roles. Unlike the trading hub scenario, there is no role reversal (as when a buyer becomes a seller in the hub model), and so the "do unto others lest they do to you next time" constraint on untrustworthy behavior does not apply similarly.

**ROLE OF THE PORTAL**

The portal operates as a pass-through facility, exposing the service provider to the client, and, usually, the client to the service provider. The portal does not intervene in transactions, and it does not aggregate the service offerings of the service providers. The portal may provide services such as common authentication services, message translation, protocol conversions, and so forth, which make certain interoperability characteristics of the service providers transparent to the service clients.

**DIVERSE PORTAL MODELS**

Portal interactions may take several forms. Interactive portals (appear to) operate synchronously with the clients actions. Portals that rely on browser-based clients are of this sort. Portals may also operate asynchronously, behaving like store-and-forward message switches. (Compare this model to the Basic Order Routing Scenario.) Hybrid portals may also exist, which operate in part synchronously, and, in part asynchronously. (Consider a portal that allows clients to monitor several services, then place transactions in an asynchronous manner. Compare this model to the Parallel Access Scenario.)

**PERSONALIZATION AND PROVISIONING**

Because the portal is a pass-through, the characteristics of the service are visible to the client, and those of the client are visible to the service. This can introduce a need (or opportunity) for each service provider to provide "personalization" capabilities for the client's convenience. Service providers may choose to offer different models of personalization. Even when the service providers behind a portal all use identical personalization models, clients may choose to personalize different services differently. This may create a need for the service provider to map the client's identity (or some representative of his identity) to a specific set of personalization values. This may require enrollment and provisioning functions, and it may require authorization or access control services to ensure that personalization values are only modified by the appropriate client or administrator.

*(End of SIMC Copyright material)*

## Additional Scenarios

The following sections characterize a number of additional scenarios. Although these are not discussed in detail, each is worthy of consideration.

### Business-to-Business

The business-to-business scenario treats businesses as entities in relationship to one another. This could include supplier/customer relationships, subcontracting relationships, collaborative relationships, and so on. This scenario takes into account the fundamental concepts of what constitutes a business and how individuals behave as agents of a business. The scenario includes a variety of interactions, including application-to-application, person-to-application, person-to-person, and application-to-person. The concepts of business exchanges and the use of independent third parties have significant implications.

### Business-to-Government

Although frequently treated as a business entity in technical discussions, the unique roles played by government – namely those of government as customer, regulator, or provider – cannot be overlooked. This scenario has significant implications with respect to privacy concerns.

### Business-to-Employee

Business-to-employee interactions are typically conducted between a business entity and an employee acting as an individual, rather than in the performance of a role as an agent of the business. Examples include employee interactions with HR systems, payroll systems, benefits systems, etc. The term is also applied to interactions with systems such as travel reservation systems, even though the travel is presumably for business purposes. In this business scenario, the different permutations should be taken into account that arise from a combination of having the employee performing these interactions from within or outside the business infrastructure, and from having the target system reside internally or on an external (outsourced) system, and any special considerations that arise when the employee is mobile. Privacy considerations are significant.

### Government-to-Consumer

Government-to-consumer interactions are usually performed between a governmental body and a citizen. The governmental body is acting in the role of either a supplier of services (e.g., US Health and Human Services), a provider of information (e.g., the Smithsonian Museum), or an enforcer of legal and tax codes (e.g., US IRS or UK Inland Revenue). The citizen is acting as a consumer of these services and information. Like the "Business-to-Employee" scenario above, the number of possible permutations of interaction could approach infinity because of the size of the citizenry and the vastness of the government bodies they must deal with – from local to state (in the US) to national, and in the case of Europe, Supra-national (the EU). Also because of the type of information that may be involved – from medical records to financial statements – the privacy considerations are very significant.

### Business-to-Consumer

The interactions that occur between a business and an individual acting as a consumer, rather than as an employee or business partner, constitute the final scenario. This scenario includes

the full lifecycle of typical business transactions, beginning with marketing, and continuing on to sales, payment acceptance, and service delivery (which may include an assortment of possibilities, such as electronic delivery of a product, tracking service associated with physical delivery, and after-sales support). Special treatment should be given to customization as it has to do with identity management, as well as to privacy concerns.

# Appendix C: Example of a Trust Model

## Architecture Principles

Architecture principles represent the highest level of guidance for architectural planning and decision-making. Principles are derived from business goals and corporate values and, within the Information Security arena, are usually presented as policies. They:

- Are high-level statements about the security that tie back to business goals

- Incorporate values, organizational culture, and business goals

- Drive technical and procedural aims

The following architectural principles are derived from studying several corporate organizations; to this end, they are an amalgam of ideas rather than the viewpoint of any specific organization. This, however, does provide the opportunity to solve a more generic problem. They are:

- Universal access is required.

- Levels of trust will be determined by corporate policy.

- All known individuals will have a single authoritative identity.

- Identity checks will be cumulative.

- Trusted identities will have a lifecycle.

- Systems access will be identity-based.

- Information access will be role-based.

- Information will be classified.

- Systems will be classified.

- Platforms must be trusted.

- Information flows must be trusted.

- A four-tier client/server model will be used.

- Personal Privacy

### Universal Access is Required

The primary aim of identity management is to establish and manage access to the corporation's information systems and data. Historically, this has meant separating employees from non-employees and establishing a perimeter around the business, restricting access to employees only.

This is no longer sustainable:

- Internet-based customers are increasing in both numbers and expectations. There is now a

requirement to provide 24x7 access to customers and to the information they require, in a real-time and personalized manner.

• There have been significant shifts towards a virtual company, with many core operations now either outsourced or undertaken by joint venture companies.

To this end, corporate assets, in the form of networks and systems, will be accessible in controlled measure to all. The aim of this is to provide a full range of state-of-the-art solutions to employees, customers, trading partners, and the general public, wherever they are located.

**Levels of Trust will be Determined by Corporate Policy**

Nonetheless, access to corporate systems and data needs to be aligned with the trust that the corporation may have in the individual. To this end, four broad categories of trust are generally accepted:

• **Totally Trusted**: This identity is trusted to access information at any level within the organization, including access to raw data or highly sensitive systems. Examples are R&D, Mergers & Acquisitions, or Information Security Systems.

• **Highly Trusted**: This identity is trusted to access information to all core business functions as determined by systems classification. Examples are Financial or HR systems.

• **Trusted**: This identity is trusted to access information to all internal systems not classified as sensitive or core.

• **General**: This identity is trusted to access only published (public domain) data.

Each identity will be able to access information at lower levels than itself, subject to having appropriate authorization.

Note that trust in identities will be ascertained by authentication systems; authorization rights will still be determined separately.

Each level of trust will have an associated policy that determines:

• The required mechanism for checking the identity

• The type of identity credential issued

**All Known Individuals will have a Single Authoritative Identity**

Using the policies outlined above will enable the corporation to establish a single trusted identity with all customers, trading partners, employees, and agents.

As rules are established for identity issuance, this activity may be delegated to trusted bodies outside the organization, such as trading partners or external trusted third parties such as banks.

As the identity ranges are cumulative, from General through to Totally Trusted, the issued identity must have the capability to be recognized by all authentication and authorization systems employed by the corporation. This is currently one of the greatest issues facing the corporation. Ideally, the credential would provide its own means of authentication and carry with it both the level of trust provided and the issuing authority (for revocation services). For the time being, the following technologies are considered appropriate:

• Customers will be offered the option of having a single electronic identity normally based

upon user ID and password. With the permission of the customer, "cookies" may also be issued to enable personalization. This identity will be managed by the corporation, or one of its agents, on the customer's behalf.

- Employees and agents will have a single electronic identity, based upon PKI technology, to enable single sign-on to all systems and electronic resources. The corporation will manage this identity.

- Trading partners will be contractually required to provide electronic identities that are compatible with both their identity issuance polices and Information Security systems. To enable flexibility, open standards will be used based on the technical requirements of the identity. Either the trading partner or a mutually acceptable third party will manage this identity. In the absence of a mutually acceptable third party, the corporation will consider issuing IDs to trading partners.

**Identity Checks will be Cumulative**

All persons accessing corporate resources will have an associated trust level determined by policy. Higher levels of trust will be deemed to be able to access lower levels of trust, with access controls to specific information provided by authorization systems. This is to allow for Totally Trusted employees to be able to access other employee systems, for all employees to be allowed access as customers, and so on.

To meet these criteria, it is essential that identity checks for lower levels of trust be incorporated into higher levels. Policies will reflect that either the same or an equivalent identity check is made.

Author's Note: This is fairly easy for organizations such as banks to implement by insisting that employees have their salary paid into an account provided by the bank. Normal banking checks will thus be made for all employees prior to more rigorous checks being made to access internal systems.

**Trusted Identities will have a Lifecycle**

Electronic identities issued by the corporation to employees, agents, and trading partners are only valid during the period the individual is either employed by, or has a trading relationship with, the corporation. When this relationship ceases, the electronic identity will be revoked.

Note that this is not normally true for general access, as the corporation cannot stipulate when a customer may, or may not, choose to trade with the corporation. It may, however, be true for customers with special status and/or subscription services; in this case the trust policy must reflect this.

- Electronic identities to be issued when the relationship commences. In the case of employees this normally means HR will issue an identity to employees requiring access to IT resources. For agents, the identity will be issued by a contracts department or their nominated agent at the commencement of the contract and set to expire at the projected contract end date.

- During the period of employment or contract, the electronic identity may lapse, be lost, or corrupted. The corporation will need to ensure that mechanisms are put in place to maintain the successful continuance of the electronic identity.

- At the termination of the relationship, the identity will be revoked.

**Systems Access will be Identity-Based**

Access to the corporation's networks and systems will require that an individual be *authenticated* via their electronic identity. This is to provide accountability at an individual level.

In particular, certain operations will require that non-repudiation services must be applied. Non-repudiation describes mechanisms established to counter an individual's denial of:

- Data transmission or receipt

- Access to information resources, such as communications systems or processing resources

- Changes to information

**Information Access will be Role-Based**

To enable organizational flexibility, access to all systems and information will be based upon role; i.e., authorization will be role-based. The resource owner will determine these access rights. Individual to role mapping will work as follows:

- HR, contracts department, or trading partner will issue the electronic identity as outlined above.

- When the electronic identity is used to access the corporation's IT resources, the identity will be verified by authentication technology and accepted as authentic or access will be denied.

- The authentic ID will be passed to the authorization technology to map the electronic ID to the current role.

- The role will be used to decide information access rights.

- The identity will be used for audit logging, digital signing, and other non-repudiation techniques.

**Information will be Classified**

Information held by the corporation will be classified as follows:

- **Public Domain**: Information published to undertake business.

- **Internal**: Information made available to employees, agents, and trading partners to enable the corporation to fulfill its business obligations.

- **Confidential**: Information that has restricted availability where general disclosure would damage the business.

- **Strictly Confidential**: Information has strictly restricted availability where general disclosure would severely damage the business.

Ideally, this information would be *labeled* to indicate the strength of the classification applied to a data item.

Classification will be used to establish the strength of trust required for access and, in particular, the authentication techniques required. For example:

| Data Classification | Trust Policy Applied | Possible Mechanism Applied |
|---|---|---|
| Strictly Confidential | Totally Trusted | Biometrics |
| Confidential | Highly Trusted, Totally Trusted | Smart Cards |
| Internal | Trusted, Totally Trusted, Highly Trusted | PKI Identity + User ID/Password |
| Public Domain | All | User ID/Password |

### Systems will be Classified

Systems used by the corporation will be classified as follows:

- **Public**: Systems are freely available for use by all, including the General Public.

- **Baseline**: Systems are available for use by employees and agents only.

- **Sensitive**: Systems are restricted to approved users only. The following types of system are likely to be sensitive: systems containing personal information; systems containing financial information; systems relating to security.

Author's Note: At a discussion amongst various corporations, the debate between classifying information and/or systems raged long and hard. There is no consensus regarding the need for systems classification. All organizations had some systems that required levels of isolation, generally relating to highly sensitive information such as Mergers & Acquisitions, R&D for next generation products, legal requirements, and staff disciplinary information or court actions. The debate is whether these systems are self-evident or whether a process can be developed to ascertain which they are.

### Platforms must be Trusted

Where computer platform physical security measures are other than standard, additional technical security measures need to be applied to ensure that overall security is maintained. For example:

- Situated on corporate premises with physical access controls, alarm systems, and attended by 24x7 security personnel

- Connectivity is to a managed Local Area Network

Outside of this standard, the three most common environments are:

- Location Independent Workers (LIW) who have desktop equipment within the home environment

- Mobile computer owners; including laptops, note-books, and Personal Digital Assistants (PDAs)

- Personnel using third-party sites where physical security may be lower

In such circumstances, the security measures applied should be aligned to those required for Confidential. Strictly Confidential data must *not* be held in any of these environments.

Levels of data classification used within most corporations do not warrant either the complexity or cost of adopting military standard trusted computer platforms or networks to maintain integrity. To this end, basic data integrity (i.e., bit/byte-level integrity) provided by applications, file storage mechanisms, databases, and operating systems is generally accepted as fit-for-purpose. However, should the need arise for higher levels of either data confidentiality or integrity, the use of a Trusted Computer Platform will be considered.

Data confidentiality will be provided by appropriate technologies determined by data classification.

**Information Flows must be Trusted**

When sensitive information needs to flow between trusted domains, the communications channel used must be as trusted as either domain. Historically, maintaining trust has meant establishing a network that handles all communications up to the highest level. This, however, is neither necessary for many information flows nor financially viable; a variety of mechanisms is, therefore, required to address needs as they occur. The ability to operate over public domain networks is also required.

Four levels of connectivity are defined:

- **Internal**: End-points reside within the corporate network and data transfer is limited to this environment. This network is trusted.

- **Shared Infrastructure**: Essentially the same as Internal, but involves an external entity. The external entity adheres to the same technical standards and security controls as the corporation. End-points reside in the overall shared infrastructure and data transfer will take place within this environment. This network is trusted.

- **Joined Infrastructure**: In this configuration, the external entity has a connection to the corporate network but does not adhere to the same technical standards and security controls. End-points reside in the overall private network and data transfer will take place within this environment. This network cannot be considered trusted and additional security controls should be applied or communications restricted to public/unclassified data.

- **Remote**: Where the external entity uses a public connection to the corporate network. This network cannot be considered trusted and additional security controls should be applied or communications restricted to public/unclassified data.

Basic data integrity at the physical (bit/byte) level is deemed to be acceptable on all networks, but additional controls should be put in place to protect data confidentiality and integrity when using non-trusted networks or where the nature of the data requires this.

Wireless transmissions should always have confidentiality controls in place.

**A Four-Tier Client/Server Model will be Used**

IT functionality will be separated to provide appropriate controls to information. A universally acceptable generic model has been adopted to achieve this; known as the Four Tier Client/Server model:

- **Client Tier**: Presentation of credentials, delivering the information.

- **Presentation Tier**: Rendering of information into a personalized format.

- **Business Logic Tier**: Applying logic that manipulates the data to provide information.

- **Data Access Tier**: Actual access to the data.

Security controls should separate each tier.

**Personal Privacy**

Individuals have a right to view and correct personal information held about them. To comply with European privacy laws, the following guidelines must be adopted:

- Individuals will be allowed to view all data held about themselves. This applies equally to employees, agents, and the general public.

- Where they have supplied the information (for example, address, phone number, etc.) they will be allowed to change this directly.

- Where a corporation or their agents have supplied the information (for example, salary, outstanding payments, etc.) the individual must be allowed to request to have the information corrected if they believe it is inaccurate.

Systems holding personal information are subject to the European Privacy Directives and must be appropriately secured.

# About the Authors

This White Paper was developed by The Open Group Identity Management Work Area. This a joint Work Area of The Open Group Directory Interoperability Forum, Messaging Forum, Mobile Management Forum, and Security Forum. It is working, in co-operation with other bodies, for a global identity management framework, by analyzing the requirements, encouraging the appropriate standards organizations to produce the standards that are needed, and helping the industry to develop interoperable products to meet those standards. Its statement of the requirements for identity management is contained in the Identity Management Business Scenario.

Skip Slone of Lockheed Martin was the Lead Author of the White Paper and managed the project. Ed Harrington of EPH Associates provided significant editing and review effort, as well as contributing material. Other major contributors were Bob Blakley of IBM Tivoli Software, Peter Harris and Nick Mansfield of Shell Information Technology International, Roger Mizumori of Waterforest Consulting, Gavenraj Sodhi of Computer Associates, Eliot Solomon of Eliot M. Solomon Consulting, and Ian Dobson and Chris Harding of The Open Group.

Skip Slone is Principal Architect in the Chief Technology Office at Lockheed Martin Enterprise Information Systems. He is responsible for establishing, promoting, and maintaining the directory and naming services architectural vision and standards at Lockheed Martin. He has participated in national and international standards development since 1988, and currently represents Lockheed Martin's interests in several committees, including the international committee responsible for X.500 and X.509, the Internet Engineering Task Force's LDAP and PKIX groups, as well as The Open Group Directory Interoperability Forum. He currently serves as Vice-chair of the INCITS T3 committee, holds the editorship of the X.500/LDAP Alignment project, and is a member of the steering committee for The Open Group Customer Council. In addition to his work at Lockheed Martin, Mr. Slone is an Adjunct Professor of Computer Science at the Florida Institute of Technology.

Ed Harrington is Principal Consultant at and CEO of EPH Associates LLC. He is Chair of The Open Group Directory Interoperability Forum and also of its Mobile and Directory Work Area. He has more than 25 years' experience in marketing, finance, and management. His company focuses on strategic management consulting for software and service suppliers and helps users evaluate and implement standards-based directory, messaging, and identity management solutions.

## About The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, whose vision of Boundaryless Information Flow will enable access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group works with customers, suppliers, consortia, and other standards bodies. Its role is to capture, understand, and address current and emerging requirements, establish policies, and share best practices; to facilitate interoperability, develop consensus, and evolve and integrate specifications and Open Source technologies; to offer a comprehensive set of services to enhance the operational efficiency of consortia; and to operate the industry's premier certification service, including UNIX certification.

Further information on The Open Group can be found at http://www.opengroup.org.

## List of Tables

## List of Figures

# Index

ABA .................................................... 59
access control................................ 16, 17, 23, 24
access control list.............................. 14
access management.............................. 75
account de-provisioning ..................... 12
account provisioning.................... 12, 13
accountability ............................... 27, 34
address information ........................... 41
affiliations........................................ 11
**ANSI** .............................................. 58
application providers ......................... 38
appraisal............................................ 34
approval ............................................ 13
architectural principles ..................... 51
Architecture Guide ........................... 65
architecture principles....................... 102
asymmetric encryption ..................... 57
attribute certificates ......................... 14
audit .................................................. 27
audit controls ................................... 24
auditing............................................. 34
authenticated identity.................... 20, 24
authentication ............... 10, 11, 20, 23, 27
authentication identifier..................... 46
authentication technology.................. 21
authority............................................ 32
authorization .................... 14, 23, 24, 27
authorization identifier...................... 46
authorization identity........................ 45
benefit assessment ............................ 21
biometric........................................... 25
biometrics ......................................... 21
BSI .................................................... 58
business audit.................................... 35
business control process ................... 27
business issues .................................. 21
business policy................................... 19
   IT .................................................. 24
business scenario ........................ 40, 75
CCITT ............................................... 57
CERN ................................................ 59
certificate policy authority................. 53
Certification...................................... 66
certification authority ....................... 53
CIM ................................................... 61
client computer ................................. 37
community......................................... 40
computer actors ................................ 36
core identity.............................. 43, 44, 70
cost assessment................................. 21
credentials......................................... 46
Data Protection Directive ................. 64

data repository.................................. 15
DCE .................................................. 46
delegated administration ................... 13
delegation of authority ...................... 9
DEN .................................................. 61
de-provisioning ................................ 14
deregistering..................................... 33
digital rights management.................. 14
digital signatures ......................... 45, 57
directories......................................... 15
directory ....................................... 5, 37
directory names ................................ 44
DMTF ............................................... 61
DNS .................................................. 43
efficiency........................................... 41
end entity.......................................... 55
enforcement...................................... 18
EPAC ................................................ 46
EURIM.............................................. 63
federated identity ............................. 17
federation of identity........................ 45
Four Tier Client/Server .................... 107
GID .................................................. 45
globalization...................................... 5
GSS-API ........................................... 56
GUID ................................................ 46
human actors .................................... 36
ID ..................................................... 25
identification ................................. 20, 27
identity .............................. 7, 10, 20, 23
   attributes ...................................... 11
   definition ..................................... 5
   verification ................................... 31
identity assurance.............................. 30
   levels of ....................................... 30
identity information........................... 41
identity information........................... 42
identity issue auditor ........................ 54
identity issuer.................................... 54
identity management.............. 5, 15, 27, 75
   architecture ................................. 28
   business value................................ 19
   standard ....................................... 29
identity management framework......... 51
identity manager................................ 53
identity owner ................................... 55
identity policy authority.................... 52
identity technology............................ 21
IdM .............................................. 5, 15
IDWG ............................................... 71
IEEE ................................................. 59
IETF ............................................ 52, 59