Identity

by

Jay Wack, President CEO TecSec, INC

July 9, 2014

Introduction

Globalization of businesses and the increasing integration of information technologies are compounded to make diversity of identity management a potential 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

Identity Management is a convergence of technologies and business processes. 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.

Establishment of Identity can be a difficult process. 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. Identity is, normally, a global event (i.e. Don is always Don). 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. Roles are, normally, a local event, under the control of the owner of the system or information being processed by that system.

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", the policy enforcement point in the enterprise. It is also the starting-point for most single sign-on environments.

The use of permissions are also fundamental to the control of, or access to, information, to services, and in the case of healthcare, electronic forms. 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.

Trust and Liability

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."

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?)

Management of risk and the issue of trust are governing progress in the whole field of e-commerce. 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 fides, 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.

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, by some, 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 analysis of a business transaction shows that multiple services are used in establishing trust. Some services are delivered by telephone, some by mail, and 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.

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.

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 or permission that has been granted. This is a process that must be properly recorded for audit purposes. 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.

Starting with the idea that trust gets translated into the notion of authority, it follows naturally that authorities become the agents of provisioning.

- 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.

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.

As identity management grows and matures, and especially as its use outside of the organization grows, the publication aspects of the directory services underlying the identity management 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 or MS Active Directory) 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.

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 identity management 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.

Without standards-based access controls and a standards-based policy interpretation mechanism, the "making decisions" capabilities required of identity management will continue to be performed, predominantly, by the application and not by the directory. Separate access controls utilize the results obtained from the directory to provide whatever permissions are available to the authenticated submitter.

Most general-purpose directories today do not function as "enforcers", but as traditional repositories – leaving the enforcement to the target application. Concepts such as "Groups", "Roles", etc. could then be much more efficiently utilized. The enforcement component could take advantage of the work done by the banking community, and as published in ANSI standards X9.69, X9.73, and X9.96.

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 can also be used to bind 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 other computers and the resources within them

- To submit forms and to electronically sign those forms

Further, the authorization component can be used as a mechanism of control to limit the specific users' access to information within a form.

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

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 an established identity. This function is managed by the introduction of a complimentary mechanism rather than using the PKI certificate alone.

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. There is also the requirement in some organizations to constrain access to information on a "need to know" basis. Although traditionally a military term, "need to know" can also refer to the individuals "justification or rational"; as in the case of patient identifiable data.

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 rights can be exerted within or by different parts of the network. Access control can begin at the login process and the network can control various accesses to applications and server locations or connections that reside within the network control. The relative owner of the information can exert further controls as it is moved through out the enterprise. This separation of control is very useful as the Network is only capable of managing access at a relatively high level, and today's information controls have fine grained access requirements to the object level (a field within a record for example).

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:

- 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 value and/or the extended permission or authorizations that have been associated with that particular smartcard and to the person the card was issued. 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. This approach is particularly useful when mobility of the user is a requirement, or where remote dialog is the norm, where the issuer and the enrolled recipient must have a level of trust maintained by the hardware itself.

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 might also 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. This is the method suggested by the Trusted Computer Module consortium to protect the installation of software to a single machine.

- *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. 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 uniquely came from that machine (or perhaps that it was authorized by the owner of that machine).

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 CONTROLS

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.

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.

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.

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
- 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). This is also defined as a security control that establishes the validity of an originator's credentials, message, or transmission.

Authorization

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). 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. Among the levels of authorization standards can be a baseline set of permissions to access, read, and modify data.

Persistent Protection of Data

A final area of concern for identity management is the provision of persistent, 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, confidentiality, and privacy, and the process, 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 in conjunction with the existing cryptographic and time-stamping mechanisms will be sufficient to provide the desired protections necessary to securely engage in electronic business communications.

Over the past few years there has been much effort to establish a mechanism for the establishment of identity on a large scale. Commercial firms have been engaged to register information about individuals and manage that information as a "neutral" arbiter. On the surface this seems like a reasonable function and business opportunity. The industry as a whole also recognized that there needed to be some overt declaration that explained and defined just what would be involved in this service. This declaration is called a Certificate of Practice Statement (CPS). However, when examined, the most a CPS can really offer is that a procedure of registration was followed. There is no possible way that any third party can vouch for a person's identity without also offering some level of assurance or liability to the action of establishing that identity. This idea of liability has, to this date, never been satisfactorily addressed. Even the most stringent examination of the reference material submitted (commonly called "seed" material) puts the examiner in the awkward position of having to be an expert on determining identity. This is made even more difficult when one considers the record keeping of different municipalities in these United States over the past 100 years. Birth certificates are available, from some States (Pennsylvania for example) over the Internet. Other States offer photo copies of a handwritten document with no official seal or validation other than the written signature of some otherwise unidentified hospital employee, or in some cases, a simple telephone conversation may be the only assurance available. Driver's licenses are routinely made available for a fee, and very little else. There are sources on the internet that will provide a drivers license for any state in the US, with any identity, combined with a very nice photo, that are accurate enough to pass as genuine to all but the most detailed, expert, examination.

What this means is that, in the final analysis, the parties must, at some point establish trust directly. Without the associated liability, trust is not transferable.

There are likely several mechanisms that can be used to establish such a relationship.

The first step is to define the objectives or requirements that must be met. The need to take advantage of the efficiencies of the Internet is clear. Time is money, and the nearly instant communications vehicle of the Internet offers not only savings in time but also in the immediacy of the response given to a request, service, or business transaction.

Registration over the Internet would be a desirable component of the solution.

Step two is to establish a trust mechanism that will allow the organizational owner of the relationship (as opposed to the members' role within the organization) to manage the relationship in a trust assuring manner that is both cost efficient and serviceable over time.

The issuance of an identity token, in the form of a smart card, or some other intelligent electronic device would be one component to consider. The issue, after all is one of identity and an identity is at the base, unique. Software can be copied, corrupted, or otherwise altered and does not lend to a high degree of assurance.

The token, as the focal point of control, would need to store, and ideally apply a unique electronic signature to a message, or be able to electronically "sign" a submitted form. Further, the token should be able to act as a "federation" device, storing the various authorizations or permissions that would be extended by the different departments or even by multiple enterprises, to that unique token and the unique individual to whom it was issued.

The token should be able to be serviced, or updated, remotely. Over time relationships change, roles are modified, privileges are extended and withdrawn, and all of these alterations need to be accomplished, in a secure manner, across the Internet.

The central issuance of the Identity Token by a given enterprise is a matter of efficiency and also logical coordination. The need for one registration process, for one individual, addressed by one token, all managed at a central site was addressed earlier in this document.

To address the problem of recourse it is suggested here that the token be sent from the central issuing facility, via certified mail, signature required, to the person to whom the token, and by extension the permissions and authorizations, as well as the token signature, has been assigned. Acceptance of, and signature on a Postal Certified Delivery, is supported by many years of legal precedence, and by Federal law.

The use of the card, under a Certificate of Agreement, can be circumscribed and the authorization mechanism (in this case cryptography) can be addressed over time, and with a very high degree of assurance, safety and relative ease.

Once in the hands of the appropriate user, the issued token offers a unique electronic signature and a stable platform that can be exercised by the insurer as well as by any other organization the issuer might authorize.

This is one possible process that could take advantage of a combination of existing technologies and laws to arrive at a cost effective managed level of trust, and still be deployable over a large population.

The authorization mechanism discussed here would allow the control of:

- The submission of any electronic data required; securely
- With persistent protection, confidentiality, and established identity of the originator.
- Differential protection at the object layer of the information submitted
- Management of the ongoing relationship, (secure post issuance of card data)
- Effective use of the Internet for two-way communications between the Issuer and the Organizational member.
- Adherence to standards and best practice guidance while recognizing the constraints of the laws and regulations that might be associated with the data.

The solution as outlined exists today. The solution consists of a smart-card loaded with the JAVA/CKM operating system, the CKM Enterprise Builder® Software for the management of the authorization component as well as the registration of the public half of the on-card generated PKI pair.

The software configuration for the use of smartcards is managed by the standard PC/SC interface found on all Microsoft platforms.

The result is persistent confidentiality of information, at the object level, making communications a matter of available connections, and storage a matter of convenience.

For more information contact:

Jay Wack

TecSec, Inc
12950 Worldgate Drive
Herndon, Virginia 20170

571 299 4107 office
301 758 6344 cell