Building Trust into e-business

"It's the equivalent of shaking hands,
looking people in the eye
and knowing you have a deal."

"The essence is to ensure that
people are who they say they are."

"Sooner or later,
all transactions will be done this way."

The Internet's unbounded opportunity for new services and electronic business (e-business) is limited by concerns about security and trust. People and institutions rightly do not trust the Internet environment to the degree that they trust today's mainstream institutions.

This report describes the cornerstones of trust needed for conducting business and personal activities over the Web. The cornerstones of trust include knowing -- who you are transacting with, that the transaction is private, that the data hasn't been tampered with, and that the participants won't later repudiate the transaction.

The foundation for creating a trusted e-business environment is to use a trusted registration process to add more reliability to the identification of participants in e-business transactions and to the authentication of their identity during the transaction process. Furthermore, the rigor of the registration process and authentication mechanisms should match the degree of trust required and the value of the transactions at stake. For example, a "soft" registration process may be adequate to create certificates that are used to identify individuals when they visit a Web site and inform them of new products announced since their last visit--because very little is at stake. A stronger registration process may be needed to create certificates that provide secure access to an individual's PC bank account. The strongest registration process may be needed to create certificates that deliver the very high level of trust needed for highly sensitive services (i.e. involving medical diagnosis) and for business-critical transactions (i.e. involving long term, high dollar value commitments).

Challenges facing e-business

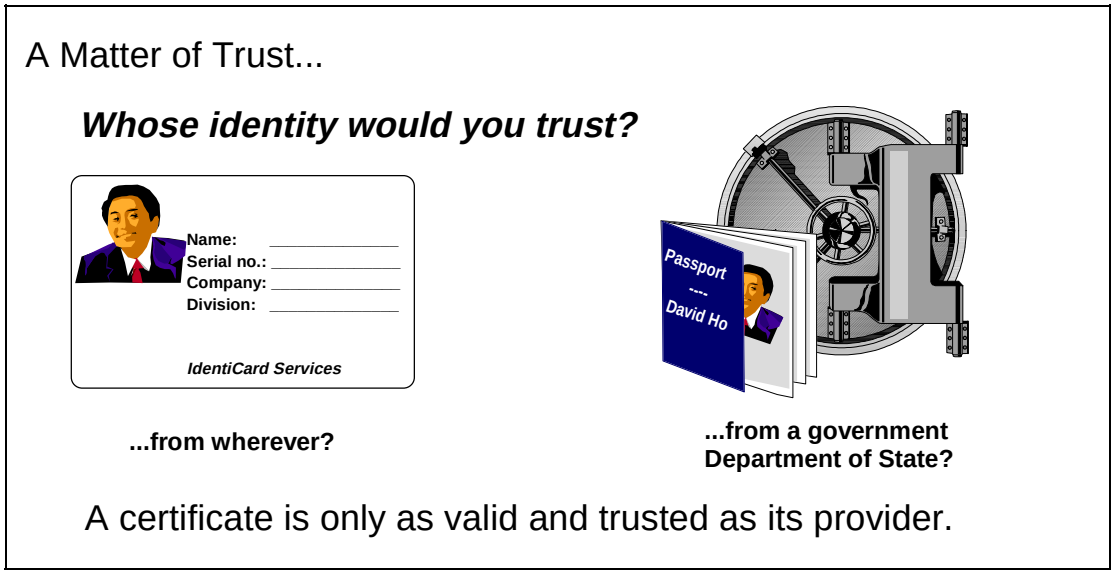
In a networked world, the requirements for trust are more demanding because:

- conventional ways of granting authority commensurate with trust rely on personal contact, which is not practical for global electronic relationships
- information for electronic transactions will likely flow through untrusted third parties.

For the most valuable e-business transactions, you can increase the amount of trust by shielding them from tampering, keeping records of their negotiation and execution, and recording them in secure online storage. This is much the same protocol that is followed using trusted, third-party custodians when the most sensitive commercial and government transactions are negotiated in a traditional manner.

Trust

Trust is at the center of personal, professional and business relationships. With trust, we can make an agreement with someone else and act on it with confidence that the other person will follow through on their end. We grant authority, responsibility and privileges depending on the degree of trust and the needs of the situation. This paradigm works well with those we interact with frequently, because we know their track record and how they will behave -- we trust them. When dealing with those we don't personally know, we trust them conditionally on the basis of their credentials and the confidence we have in the person or institution that issued the credentials. For example, a passport is more trustworthy than a birth certificate, and medical board certification is more trustworthy than a degree.



This paradigm can break down as the circle of those we make agreements with expands. The primary purpose of many inventions and institutions has been to foster trust in a widening circle by recording the details of an agreement and providing mechanisms to enforce agreements. Consider the inventions of writing, accounting, contract law and the court system.

Needless to say, we often have to transact with those we don't trust. In those instances, we rely heavily on any and all tools, techniques and technologies that can reduce the risk of undesirable outcomes from our interactions. Especially important is the ability to extend privileges in a controlled fashion so that the credentials we issue grant only the degree of authority required for the task at hand.

The Internet and other data networks have dramatically expanded the circle of those we can engage in transactions with, but this has happened so quickly that business practices and technology haven't kept pace to provide the level of trust in online venues that we are accustomed to from our mainstream institutions.

Facets of Trust

The facets of trust can tell us what is needed in a networked application to deliver controlled degrees of authority and privileges needed by participants in the extended organization: customers, suppliers, business partners, employees and other stakeholders.

The key facets of trust are to establish, maintain and protect a trust relationship. These facets lead us to the types of trust and other requirements needed in a platform to support trusted e-business. In addition, we see that although the terms are different, the underlying function and role played by a trusted e-business platform is equivalent to what happens in day-to-day life.

Establish Trust

A trust relationship often begins with a personal introduction, a meeting. The parties get to know each other, discuss the problem at hand and describe relevant training or experience. In the world of networked applications, there may not be time or a convenient place for an in-person meeting. Instead, there is a process, Registration, that can play a similar role. Registration takes many forms, but generally the person (the Applicant) who wants a service or some other specific privilege or entitlement, applies to a Registrar or Registration Authority (RA).

The Applicant provides information to the RA. The RA checks the information to the degree deemed appropriate given the credential being requested to confirm its verity with available document sources or trusted third-parties who are already familiar with the applicant. The RA evaluates the application to see if it fits the requirements, policies and guidelines used for the certification process. At the same time, the applicant may have already checked the credentials and reputation of the RA to confirm that a certificate from the RA would be useful.

Assuming registration goes smoothly, the application is approved and sent to an affiliated Certificate Authority (CA). The CA, based on the RA's approval will, for a defined period of time, "vouch" for the applicant, if asked, to a certain level or for a defined purpose. The CA performs vouching by issuing a certificate to the applicant. Information in the certificate may also be logged and stored for controlled online access by other authorized applications for later verification. The certificate summarizes the rights and privileges associated with the credential or entitlement. For example: "entitled to deposit and withdraw funds from account 123-456-789 at the ABC bank" or "is authorized to issue purchase orders for up to $100,000 on behalf of the XYZ Corporation."

Most registration and certification processes are performed in accordance with defined procedures using strict evaluation criteria. It is vital that electronic registration be performed with strong technological safeguards and with at least equivalent procedural safeguards.

Maintain Trust

There are many ways that we maintain others' trust in us. Most involve living up to the agreements we make. In the networked world, it's very similar. From time to time, we apply to extend our certification and provide evidence of our recent performance and ongoing activities.

The RA again reviews our application, checks it and instructs the CA to extend or reissue the certificate. As before, the CA sends the extended or new certificate to the applicant and publishes it on the network.

What happens if the trust is broken? In the day-to-day world, the board that granted a certificate can revoke it for cause or because the holder failed to apply for an extension. The same can occur in the networked world. In fact, we can expect to see side-by-side print AND network publication of certification events.

An important role for RAs is to follow up on outstanding certificates and to revoke those that have expired or need to be rescinded for cause. As with any certification board, it is important to have a good maintenance process that will stand up to challenge and to follow it scrupulously. Underlying the maintenance process there must be a robust technology infrastructure that helps protect against hacking of the RA's work-in-process and the CA's certificate directory. Ideally, this infrastructure would employ security procedures to isolate each registration role and work process so that the registration process itself is shielded from technological assault.

Protect Trust

At the heart of protecting trust relationships is taking steps to ensure that unscrupulous people do not act in our name and misuse the privileges we have earned. In the day-to-day world, we safeguard our driver's license and give out our credit card number only in "trusted" situations. In institutional life, we separate duties, grant specific authority and privileges and enforce accountability. For example, the ability to sign binding contracts of certain dollar ranges is granted only to specific company officers.

In the networked world, institutions need similar mechanisms to grant specific privileges to individuals (or other entities such as computer programs). The mechanisms generally need to be effective across the globe. In practical terms, the user's evidence of trustworthiness, the certificate, has to be verifiable from anywhere in the world and the system providing the verification has to be universally recognized as reliable, trustworthy and effective. In turn, this means that the systems which publish and verify user certificates need to support inquiry over the Internet or private networks.

Registration and other e-business applications should be designed to clearly isolate roles and privileges with mechanisms to enforce the isolation.

There is a range of standards-based technologies that work together to help establish, maintain, and protect trust in a global, networked environment. The catch phrase for these standards is the Public Key Infrastructure, or PKI.

The nature of trusted applications is evolving from small individual trusted and secure applications to full horizontal and vertical integration offering a variety of trusted services. As a result, institutions should be prepared to migrate their security solutions from certificate servers to embedding PKI capabilities into broad applications.

Trusted e-business

e-business is about transforming the way key business processes are done by using Internet technologies. Critical to trusted e-business is the ability to extend trust from the organization to its employees and agents. The ability to do this depends not only on the reputation of the organization but also the reputation of the technology and service providers used to extend the web of trust.

An important factor is that networks, themselves, introduce a new environment that necessarily includes untrusted intermediaries. For example, the medical insurance form you fill in online or send by email may float through a dozen network routers in as many states, and could be copied by the unscrupulous.

To gain the benefits and cost savings of networks in applications requiring trust, we need to incorporate standards-based PKI technologies into our extended applications to attain the levels of trust needed by the application and adapt our institutions to work with digital security technologies. The security cornerstones for fully trusted e-business include:

- access control – a mechanism to prevent untrusted users from using the application or getting to the information
- transaction privacy – a way to keep uninvolved parties from reading the information, even if they gain access
- information integrity – a means of informing recipients if a message has been tampered with
- authentication – a way to allow recipients to readily identify their transaction participants and correspondents
- non-repudiation – a way to guard against having the parties to the agreement later disavow themselves from the transaction.

==========Overview of Security Cornerstones==========

In the digital world, there are five types of security that together make trusted e-business possible.

--Access Control-- *Are unknown or untrusted users prevented from using an application or accessing information?* Access control is a mechanism for limiting the use of a specific resource to authorized users. The most common form is to require users to supply a secret password before the application opens or data is displayed.

--Transaction Privacy-- *Is the personal information I give out being compromised?* In the past, transaction privacy resulted from use of shared secret keys and private networks. Shared secret keys are impractical for large organizations, and keeping the network private limits the benefits of global access and contact. Transaction privacy typically involves the sender encrypting the message using the recipient's public key to keep sensitive information scrambled and unintelligible. The recipient uses his or her corresponding private key to decrypt the information and thereby makes it intelligible. Each user has only one secret key, not dozens.

--Information Integrity-- *Am I confident that the data I receive and send is not being tampered with?* Information integrity provides a way to determine if the contents of a message were tampered with after the message was digitally signed by its sender. The signing process computes a short message "hash" or digest, which is saved with the message before it is encrypted with the recipient's public key. When the recipient decrypts the message with his private key, his system then recomputes the message digest. If the two digests are equal, then the recipient knows the message is unaltered.

--Authentication-- *Is this person who he says he is?* Authentication helps ensure that participants in an electronic transaction are who they say they are. The process of signing an electronic document involves encrypting the senders name and other information with the senders private key to create a signature block. The signature block is appended to the message and both are encrypted with the recipient's public key before the message is sent. When the recipient decrypts the message with his private key, his system then decrypts the signature block with the sender's public key. If the signature block is decrypted successfully, then the recipient knows the sender's private key was used and can thereby assume it was created by the sender.

--Non-repudiation—*What evidence is created to counter attempts by an entity that issued a command from denying that the command was actually issued?* Non-repudiation helps protect the validity of a transaction. Non-repudiation results from a combination of Public Key Infrastucture (PKI) measures, including use of an encrypted digital vault to hold records of the transaction and digital timestamping to document when documents were signed or otherwise processed.
==========

Applications can attain the level of highly trusted e-business gradually by starting within existing trust frameworks, and then using appropriate technologies and practices suitable for moderately sensitive applications.

Within Existing Trust Frameworks

There are many situations where use of the Internet or an intranet fits within an existing framework of trust. Trading partners, for example, increasingly use a private network to exchange what formerly were paper order forms, payment promises and shipment schedules. Some organizations follow up transactions with paper records to provide a conventional paper audit trail. As long as the relationship stays within the existing secure framework, the necessary security features include access control and transaction privacy.

Access control is provided by passwords or PINS which identify a user to an application, server database or operating system. Unfortunately, passwords can be readily compromised because multiple people (and systems) need to know the password or handle it in the course of operations, including: the user, the administrator who issued the password, the application that validates the password, the file or access control list and backups that contain the password, the secretary who was given the password, the Post-it, diary entry or file that the user maintains with all the passwords, the conversion file for single sign-on support, as well as any person who intercepted the mail or network transmission.

Clearly, passwords do not give users complete control over access. This may be acceptable in a closed loop system where other mechanisms, such as a private network, are controlling access to the application. When users are granted access to the application through a public network, passwords are usually insufficient and more robust security is needed.

Transaction privacy is provided by encryption keys and use of private networks. Encryption keys are used to encrypt (scramble) and subsequently decrypt the message. The users share the key. There is no problem sending an encrypted message because any untrusted intermediary can't understand it even if they do copy it. However, there needs to be a mechanism for distributing the shared secret key. The secret key could be distributed over the system, by phone, physical

mail or any other mechanism. The problem with a shared secret key system is, with multiple users, there are many keys to maintain: one key for two users, six keys for four users, 45 keys for ten users, and so on --which is impractical, burdensome and in itself a security risk.

Private Networks are one of today's principal privacy mechanisms. An organization can protect resources by not allowing network access. The major flaw is that often, malfeasance is done by people in the organization who already have or can get unauthorized access to information and applications. Also, what happens when members of the organizations need to communicate "outside" of the organization? Demands by customers for browser access to product and account information and by mobile employees to company data are forcing private networks to open up. This leads the organization to use gateways, routers, and firewalls to control the traffic entering and leaving the organization's private network. These need to be carefully managed by highly skilled people in order to maintain security and trust.

For Moderately Sensitive Applications

The exploding use of the Internet centers on situations where the level of trust needed or the transaction value is only moderate. In other words, the consequences of compromise are limited or contained. Examples include on-line access to non-confidential information, or small-scale retail / wholesale purchasing. Safe conduct of moderately sensitive applications requires the same security features required for existing trust frameworks: access control and transaction privacy, plus information integrity and authentication because the Internet is an open medium and you can be contacted by anyone.

Information integrity comes from confirmation that the message hasn't changed since the moment it was signed and sent. Authentication is used to identify the person (or entity) who signed the message.

For Highly Sensitive, Business-Critical Applications

The real benefits of networking will be limited to moderately sensitive applications until the strength of security solutions expands to 1) grant specific privileges on a global basis, 2) protect transactions even when they flow through untrusted, third-party intermediaries, 3) maintain auditable records of important transactions, and 4) hold business-critical information and digital documents in secure, online repositories.

Possible untrusted intermediaries include: a temporary worker assisting with a project, the staff of the organization's Internet or regional backbone service provider, a systems administrator in a financial institution or a clerk at an insurance broker. Whether a secure online repository is sponsored by the transacting agency or a third party, users need to feel that the important information they entrust to the repository will be safeguarded.

People are rightly concerned about transacting substantial value (e.g. stock trading, home banking, check clearing, etc.) or safeguarding high levels of trust (e.g. sharing medical records, receiving credit information, etc.) when there is a chance that the information or transaction could be intercepted and misused. In most highly sensitive applications, there is a need for

storage security throughout the life of the negotiation and the ensuing contract or transaction. Safety of highly sensitive applications requires the security features of moderately sensitive applications, including access control, transaction privacy, information integrity and authentication, plus non-repudiation.

Techniques to support non-repudiation include: 1) performing any registration or certificate processing, including authentication and the transaction, itself, in a verifiable and secure manner, 2) assigning roles and privileges in the handling of a transaction to specific individuals and applications, 3) storing the agreement as well as record of its signing in a secure archive, and 4) maintaining audit records of transactions that document its handling and identify attempts of tampering by dishonest third parties. In addition, support for non-repudiation will get stronger as the number of jurisdictions that pass so-called "digital signature" laws increases. Such laws expressly allow digital signatures to be used like physical signatures.

In short, **Trusted e-business** is about providing ways for highly sensitive transactions and services to be made over a network and computing infrastructure that includes untrusted intermediaries. Furthermore, the techniques and technologies used in trusted e-business should enable participants *to conduct trusted e-business in a complex environment in which the disparate parties may not necessarily trust each other and need the ability to precisely control the privileges they grant each other*.

Past Security Measures -- Now Inadequate

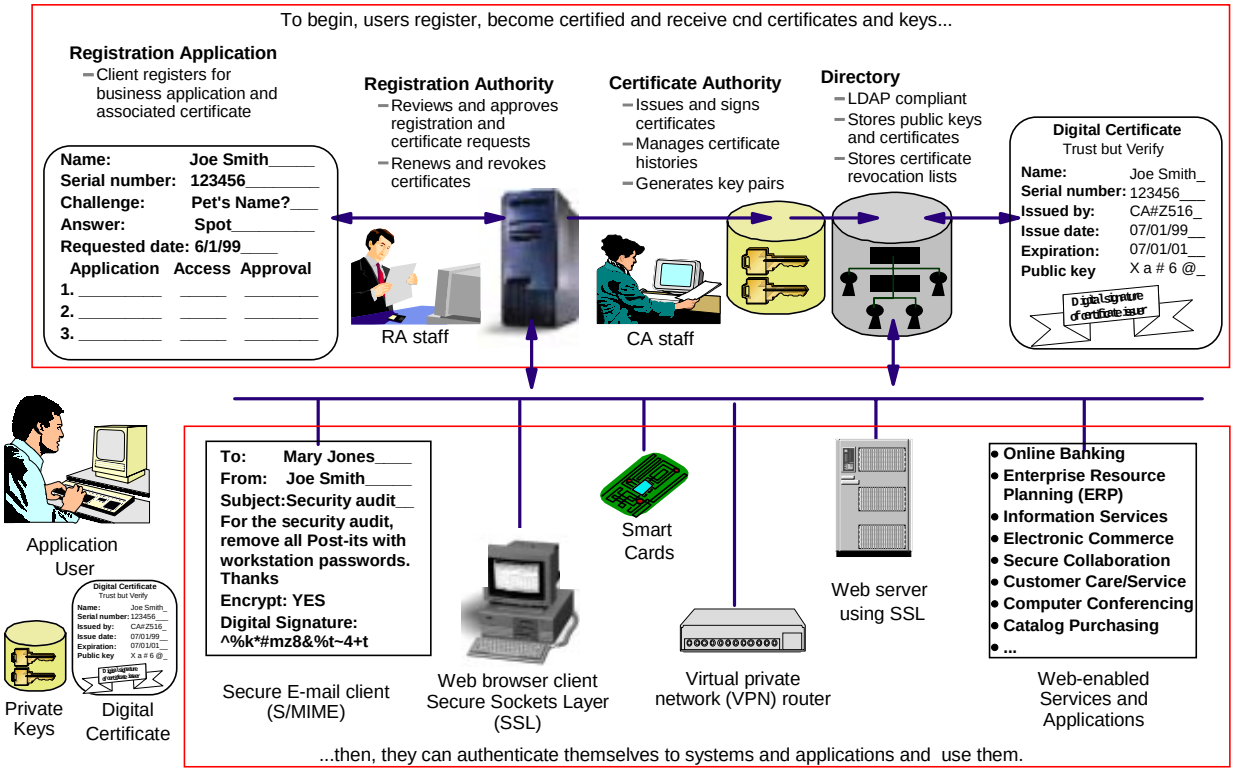
In the past decade, the security cornerstones were addressed by paper audit trails, passwords and PINS, encryption (using a shared secret key), and private networks. In many instances, especially for moderately sensitive applications, these were sufficient to conduct business electronically. These common techniques are now inadequate to provide trusted e-business for highly sensitive applications on a global scale.

Digital Certificates and the Public Key Infrastructure

Public Key Infrastructure (PKI) technology is the catch-phrase for a leading, standards-based trust mechanism for electronic commerce and other business transactions over the Internet. By using PKI and isolating individual roles and privileges in application design, organizations can design and implement a trust model that grants only those privileges needed by specific individuals or entities.

PKI technology provides the tools and means to build such a trust model. It is the responsibility of the business sponsor to determine the degree of trust required and the roles and privileges that properly distribute the trust. It is the responsibility of the security architect and the developer to use PKI features to implement applications that embody and enforce the trust model. PKI capabilities can then provide and manage credentials, certificates and keys required by the application. A critical advantage of PKI over predecessor security technologies is that end users need to keep track of only one (their own) secret key, not multiple shared keys. PKI security technologies such as encryption, signing, authentication, timestamping and network X.500 directories work together to provide a comprehensive security infrastructure.

PKI Enables Trust Across the Extended Enterprise



- *Certificates are issued to users and sometimes devices and applications to enable authentication.*
- *Private keys are issued to users for message decryption and digital signature functions.*
- *Public keys are obtained from the directory for message encryption and signature verification.*

PKI functions include:

Registration Authority (RA) is an organizational function that uses the organization's policies and procedures for establishing trust relationships and issues certificates to applicants based on their credentials. The RA, by evaluating credentials and evidence, vouches for the association between the individual and the record of his identity, which is the basis of the CAs issuance of a public key.

Registration Application is the set of procedures, software and systems that enable the ultimate end users to register for a business process. Web-accessibility is an important feature that can enhance usability and convenience of the registration process, which ultimately makes it easier for a wider audience to register to use the business system. The Registration Application enables the user to interact with the RA, and is often the means by which the digital certificate, issued after RA approval, is returned to the user.

Certification Authority (CA) provides digital credentials to participants and related products and services that use these digital credentials to provide overall access control, data privacy,

information integrity, authentication and non-repudiation. On a day-to-day basis, the CA is the trusted party that vouches for the association between the individual and his public key.

Digital Certificates are network accessible records of the user's privileges. A certificate holds the user's public key and provides the certificate holder's privileges in response to a network or user query. The digital certificate is the mechanism that enables third parties to authenticate an identity record with the trusted CA and thereby verify the rights and privileges granted to the holder of the identity record.

Digital Signatures identify the holder of the private key used to digitally sign a message and confirm that the message hasn't been tampered with. Digital signatures use keys and encryption algorithms to ascertain whether a message has been changed since the time it was created.

PKI makes it easy for end users to employ advanced security measures of encryption and digital signing. Browsers and end user PC software help to perform these functions. If encryption is needed, the user encrypts the message with the public key of the recipient and the recipient decrypts the message with his corresponding private key. If signing is needed, the sender signs the message with his or her private key and the recipient authenticates the signature with the sender's public key from the network directory.

Opportunities for new types of applications

There are many opportunities for trusted e-business applications. The common features of trusted e-business applications include:

- Registration of users, parties to agreements and the systems handling the transactions themselves. Staff of the Registration Authority applies the registration policies and makes registration decisions. The registration process must be defensible against compromise.
- Issuance of certificates to users, publication of certificates in a network-accessible directory and update and revocation of extant certificates. Staff of the Certificate Authority handles the technical and administrative tasks of issuing and managing certificates.
- PKI-aware applications that use certificates as the basis for granting access, maintaining transaction privacy and information integrity, performing authentication and supporting non-repudiation arguments.
- The application should support clear separation of roles and privileges, minimizing potential for compromise of security by unauthorized individuals.
- Audit records to enable after-the-fact confirmation of the transaction and to detect any tampering attempts.
- Physical or logical 'vault' facilities to archive signed agreements and in-process transactions with security to support non-repudiation arguments.

See the Applications by Industry section in the Appendix for examples of trusted e-business systems.

Considerations for Implementing Trusted e-business Solutions

Drivers

Government Regulations: Government regulations are very important for trusted e-business. Many states have passed or have pending digital signature legislation that will govern many important aspects of e-business. This legislation can help foster applications such as: Digital Insurance Policies, Digital Financial Instruments, Digital Wills, Digital Notaries and Digital Timestamps, to name a few.

In addition, Federal agencies are looking at e-business on a more global basis to ensure that safeguards are in place. Some of the agencies considering instituting controls are the SEC, IRS, DOD, GSA, SSA and others. These agencies may in turn place controls on how an organization operates in the e-business world.

Industry Mandate: Industry mandates come in different flavors: 1) to continue to be sanctioned by an industry association, the business must comply, 2) compliance has a defined price per transaction, or noncompliance carries a tax, and 3) non-complying businesses must deal through a complying intermediary.

The company is experiencing security violations (and related financial or public relations losses) from an internal MIS group or external service provider or is very sensitive to this issue from past experience, trade journals, etc.

The organization's e-business transactions are high-valued, and greater non-repudiability support is important.

The company's customers and other stakeholders are sensitive to end user concerns about privacy of sensitive user information exchanged as part of the e-business application.

The organization knows that centralized control delivers high security economically. To maximize security and minimize total expense, many corporations and Federal or State governments expect to set up a single secure dedicated operation to run their PKI solutions and to lease this service out to all the organizational divisions.

Service providers who wish to run multiple trust environments in a single operation. Service providers may provide services (e.g. RA and CA services) to multiple organizations that do not trust each other, and may even be vicious competitors in the market place. This requires a security solution that supports multiple CAs within a single enterprise, or multiple private-labeled CAs operated by a service provider.

Consortium. Similar to service providers, consortia need to provide a registration, certification and authentication service that operates on behalf of its members.

Readiness

Implementing trusted e-business applications requires a commitment to identifying the critical business processes that must be highly trusted, and the roles and associated privileges of different participants. After that, a PKI infrastructure can be designed and established to support the e-business.

If **Registration** of customers, business partners and applications is viewed as a critical trusted process that is a prerequisite for expanding the e-business, then a flexible registration process is required.

When a highly sensitive e-business application has already identified, then the organization will likely need a combination of integrated security features and the development flexibility to support it -- reducing the time and skill requirements for developing a “home grown” solution.

If the **business benefits** of investing in the solution have been identified and analysis indicates the project has an attractive ROI, then long term scalability and viability are critical selection criteria. Examples of typical business benefits include:

- Increased revenues because of greater market penetration
- Enhanced information privacy for end users and the business
- Reduced marketing costs because of passive selling
- Acquire Internet users from marketing campaigns
- Reduced fraud (financial, authentication, intellectual property)
- Reduced paper volume because forms come in electronically
- Increased customer satisfaction (resulting in greater sales)
- Increased employee productivity and morale especially for mobile employees
- Reduced mail room volume, mail and courier costs
- Faster transaction times (resulting in improved customer service)

When **competitive pressures exist,** a flexible and comprehensive PKI security platform can help the organization maintain the security edge necessary to compete successfully in an untrusted environment.

Technical Considerations

Standards-based. The nature of security platforms is that they need to integrate with PKI solutions in counterpart organizations (trading partners, etc.). Consequently, the security planner should look for a standards-based solution that is designed to interoperate with other standards-based applications.

Integrated components. Customers wishing to operate their own Public Key Infrastructure, such as registration, certification, certificates and directory need a solution in which the components are already seamlessly integrated. This reduces the cost and complexity of assembling such a system from multiple vendor offerings.

Application re-engineering and PKI integration. Applications will need to be enhanced or "front ended" to perform the certificate validation function to grant access. In some cases, an

application can be re-engineered to support the PKI infrastructure to enable transactions among a diverse user group. It is the application's responsibility to determine whether or not to accept a Digital Certificate and act on the privileges it contains. Applications may also have to verify specific certificate extensions designed to implement roles, privileges or other application-specific requirements. Any data contained in the Digital Certificate will need to be interrogated by the application, especially if extension fields are utilized.

Flexible security requirements. Validation of a user's certificate requires access to components depending on the specific security requirements of the application. In a simple case, a Web server can validate the certificate by checking the expiration date in the certificate and then validating the organization signature on the certificate with the public key of the organization's Certificate Authority. In many cases, the server would also need to access a Certificate Revocation List (CRL) to see if a user's privileges have been revoked. In some cases, the application may look at a directory, authorization table or Access Control List (ACL) to see what specific privileges the user has.

IBM Vault Registry

Overview

IBM Vault Registry is a robust, integrated solution for managing the registration and certification of parties conducting trusted e-business transactions. It is a high security, integrated RA, CA and user registration solution that utilizes an X.500 directory to help enable organizations to conduct sensitive, high-value transactions over the Internet and Intranets.

IBM Vault Registry implements an **enhanced trust model** that greatly improves authentication, privacy, and non-repudiation among transacting parties by shielding the transaction from any unauthorized intrusion, both internal and external, including service providers and operators/ administrators of the system. The integrated RA and CA features help reduce the overall complexity and cost involved in implementing and managing the certification process.

IBM Vault Registry addresses the business requirement for improved security of the registration transaction and end user concerns about privacy of sensitive personal information provided in applications (social security number, credit card number, etc.) by

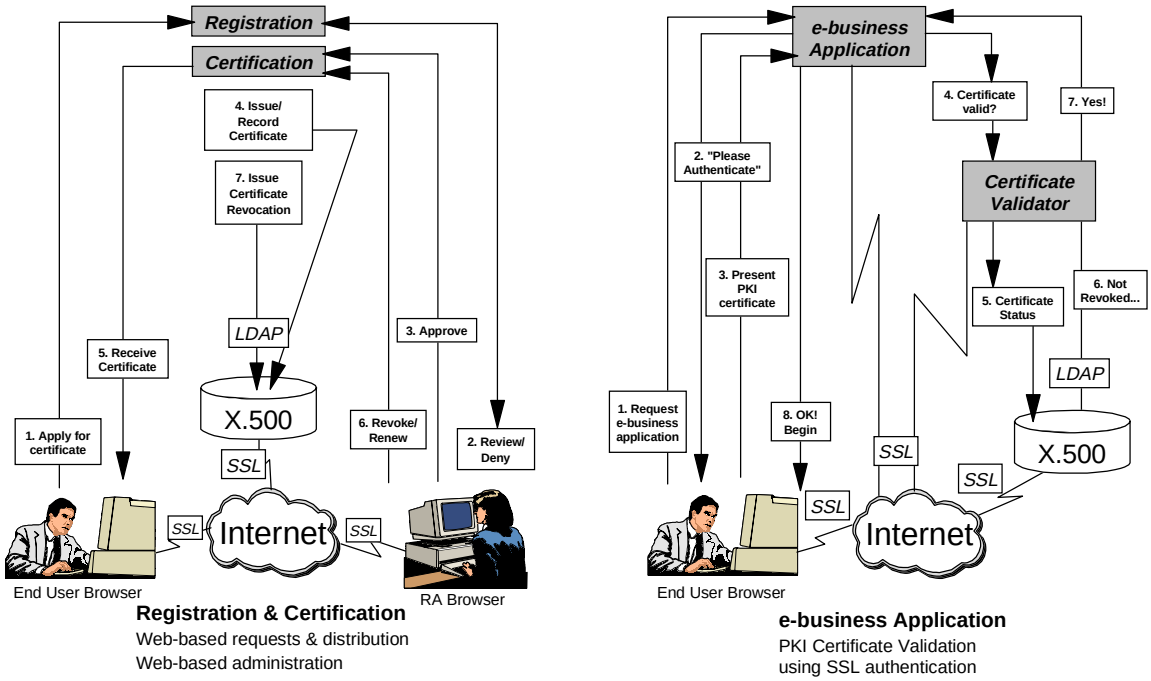
- Protecting "secret" registration information (details disclosed by applicants used for authentication, such as family names, work history, salary, health conditions, account numbers, etc.) from falling into wrong hands who could then successfully claim a false identity. Vault Registry provides the registration application that creates a trusted environment for applicant data submission on the Web using Secure Sockets Layer to communicate entry forms from the user's PC to the RA.
- Protecting against entities other than the designated RA being able to access and fraudulently authorize applications. Vault Registry provides a trusted environment for registration using encrypted electronic vaults to protect the registration process, itself, from unauthorized access.

Architecture

IBM Vault Registry enables trusted e-business applications on the Internet by providing a robust, integrated, security-rich solution for managing the registration of and issuance of digital certificates to trusted entities. IBM Vault Registry provides integration of an innovative 'vault' server (the IBM Vault Controller) that runs applications on behalf of authorized users using certificate based authentication; a flexible RA application that runs on the 'vault' server; a robust certificate management system; an X.500 directory repository for storing certificates and certificate revocation lists; IBMs award-winning DB2 database; and Lotus Domino Go Webserver, to provide a solution for organizations in the business of, or enabling others to be, a Certification Authority (CA). The solution relieves customers from the cost, time, and complexity of building ground-up from non-integrated offerings from multiple vendors.

IBM Vault Registry is designed to help enable customers to run business-critical applications on the Web. IBM Vault Registry implements an enhanced trust model that reduces the risk of compromise to the integrity, authenticity, and information privacy of Web based applications. Application transactions are shielded from unauthorized third party intrusions, both internal and external, including systems administrators, and operators. Using digital certificates for authentication and access control, data is protected in "personal vaults" against unauthorized disclosure and vault applications are protected against unauthorized execution.

Secure Registration and Robust Certificate Management Enable Trustworthy Applications



Advanced e-business applications should utilize secure user registration with revocation/ renewal processes and robust certificate issuance and management to ensure parties in a transaction are authenticated and authorized.

Real-time certificate validation provides confidence that online business can be conducted with even more trust than physical-world business.

Registration Application

The IBM Vault Registration Application Facility is a flexible registration facility for users, RAs, and servers. Users can apply to the RA for certificates using a Web browser. The Registration Application is a management application for Registration Authorities. It integrates the certificate management system, global directory, and the Domino Go Webserver -- providing a comprehensive system for public key registration processing over the web. It is a full-featured offering that includes auditing and reporting services for registration transactions, and is enabled for remote monitoring as required for a highly available services environment.

IBM Vault Registry's flexible RA implementation includes support for multiple RAs, manual or automated RA approvals, and the ability to use out-of-band verification steps like personal interviews, references or checks against third-party databases. The flexible registration processing includes "policy exits" that allow for specification of certificate attributes, automated verification checks against legacy databases, synchronization updates to various company databases, and other actions as dictated by the customer's business policies

Certification

The IBM Vault Certificate Management System provides the functions that enable organizations to set up their own CA and issue X.509v3-standard digital certificates to its authorized users (or other entities), allowing enterprises to confidently deploy their offerings over untrusted networks. An enterprise can use certificates to protect its information, applications and users from external and internal threat.

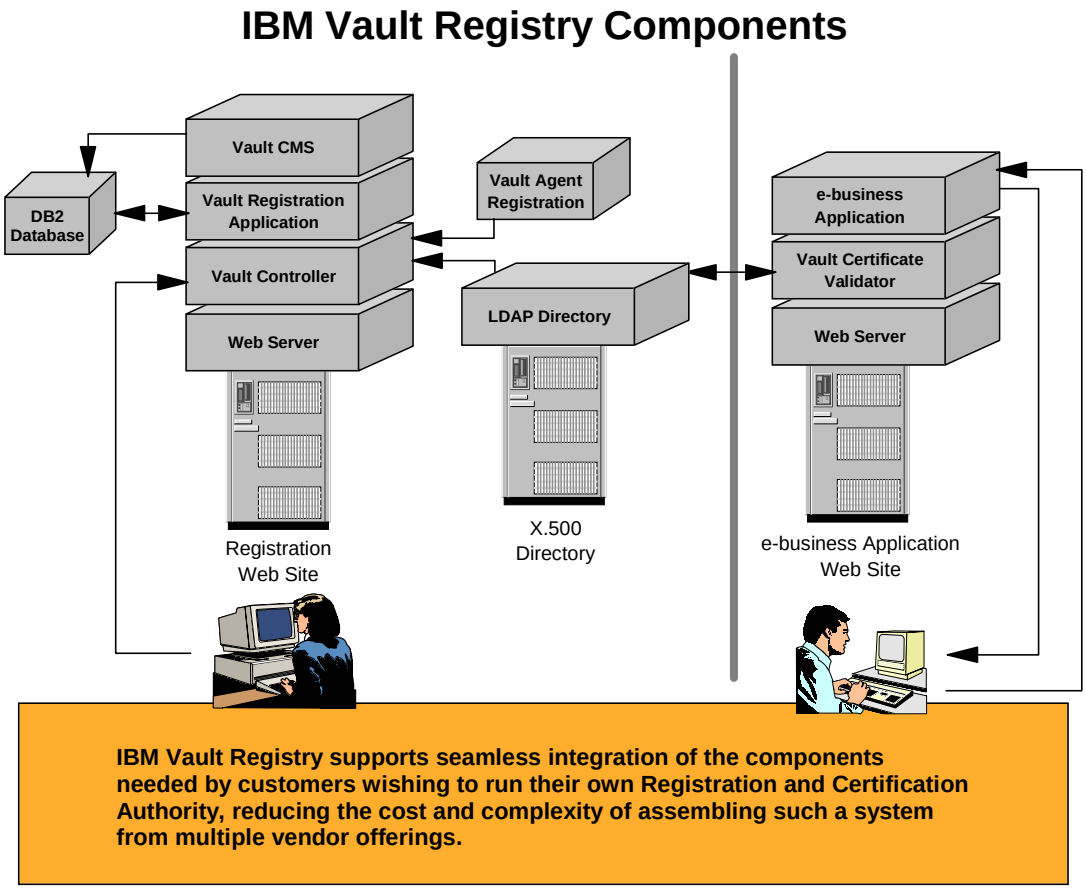
Vault Registry's flexible CA implementation can seamlessly integrate a certificate management system, optional cryptographic hardware (if needed) for added key security, an easily customizable registration application, a proven X.500 directory for storing and validating certificates, and IBM's award-winning DB2 database and Lotus Go Webserver. Together they provide a security-rich and comprehensive CA solution - all from a single source.

IBM Vault Registry Solution Components

IBM Vault Registry addresses a variety of customers concerns associated with conducting business over the Internet. The individual components, taken together, create an environment of trust and security in which customer-developed e-business can be conducted safely and with privacy for the enterprise and the individual.

The **IBM Vault Controller** is an enhanced Web server built on Domino Go that provides "personal vaults" for users, RAs, and CAs. A personal vault provides a security-rich environment for executing programs and services on behalf of a user. Personal vaults, and their contents, are accessible from SSL-enabled Web browsers that contain the corresponding vault certificates.

Access to personal vaults requires a vault certificate and digital encryption key. Information stored in personal vaults is protected against disclosure to unauthorized persons (e.g., system administrators and other vault owners) by encryption, against tampering by digital signing, and against untrusted communications with unknown parties by using digital certificates. Information can also be transmitted to other vaults using encryption, signing and certificates for security. Organizations need such a high level of security because their registration forms usually require customers to provide sensitive or personal information.



The IBM Vault Certificate Registration Application is a Vault Controller application that enables organizations to register users for its services, and administer the issued certificates over their life cycle. The application is written to be very flexible, allowing organizations to easily customize the registration pages and the policies associated with the registration process.

The **Vault Certificate Management System Facility** (CMS) enables a CA to issue, renew, and revoke X.509v3-standard certificates. Additionally, the CA publishes certificates, Certificate Revocation Lists (CRLs), and policy information to an X.500 Directory.

The **IBM Vault Agent** is a distributed vault process designed to run remotely from the IBM Vault Manager. It incorporates a small subset of the Vault Manager functionality. This subset enables the Vault Agent to exchange encrypted messages with vault processes running under the control of the Vault Manager. For example, organizations can use it with the Automated RA vault process to request and receive certificates for their customers and employees with a high level of confidence depending on the type and size of encryption keys being used.

The **IBM Vault Certificate Validator** allows remote servers to query the X.500 directory to check revocations, request certificates and to confirm their validity.

Benefits of Vault Registry

Vault Registry meets the demanding requirements of many customers based on a new paradigm that assumes that transactions will pass through an untrusted third party and that encrypted storage is required on the network to handle in-process and pending transactions and thereby provide support for a higher level of non-repudiability. Vault Registry provides a Web-accessible registration application that enables end users to register for business processes and interact with the Registration Authority during encrypted sessions. IBM has the resources and reputation to deliver and provide solution integration and ongoing support.

While most web based CA solutions use SSL encryption to protect application data during transit, the security does not extend to the server itself. Data on the server is often "in the clear", accessible by administrators and others with the right passwords.

IBM Vault Registry provides an end-to-end security solution by extending registration security to the server. IBM Vault Controller software allows the registration application used by the RA to run in its own trusted vault as a separate process running on behalf of the RA, isolated from other users as well as administrators. All data sent to the RA is held encrypted on the server in a user's personal vault, accessible only to designated RAs upon successful authentication using digital certificates. In addition, all RA actions are logged to permit after-the-fact review.

With other vendor’s solutions, an X.500 directory must be often separately sourced and integrated, a registration application developed from scratch, and a database product separately sourced from a database vendor - all at considerable expense of skilled resources and time.

Operational Characteristics

Vault Registry provides flexibility to address real e-business requirements, including integration with legacy databases and the ability to customize the registration process to the customer's unique business policies.

Its high availability and serviceability, includes support for robust, high-availability operations including service bureaus. Capabilities include continual monitoring and auto-restart of critical processes, remote delivery of exceptional system events, extensive logging and reporting support, and tools and procedures that address system-wide recovery and integrity in the event of failures.

For service provider environments, IBM Vault Registry provides a highly scalable solution supporting multiple CAs per machine, and easy boarding of new customers by allowing rebranding and customization on remote servers.

Vault Registry offers the flexibility to customize the registration process for unique business policies and ease of use, and is designed to integrate with back-end systems to protect and leverage investments.

Usage Scenarios

IBM Vault Registry can play a vital role in the delivery of business and governmental services, delivering improved customer service, efficiency and security. See the Usage Scenario section in the Appendix for a representative example.

Summary

IBM Vault Registry infuses trust into the extended enterprise by allowing e-business transactions to travel across organizational boundaries with privacy, security and confidence. Vault Registry also provides encrypted, on-network storage for applications that require recordkeeping security throughout the life of the transaction or business relationship. This recordkeeping security is critical for rebutting repudiation attempts, agreements that signers wish to unilaterally renounce.

==========Reasons to Use IBM Vault Registry==========

A secure registration process helps ensure that digital certificates are worthy of trust. IBM Vault Registry's advanced registration application uses encryption and digital signing to provide confidence that online business can be conducted with even more trust than physical-world business by enhancing the security and integrity of the registration business process that is used to identify and authorize parties in a transaction.

Innovative "vault" software helps protect data and applications from disclosure to unauthorized users. The IBM vault software uses encryption for isolating data and applications by responsibilities and roles - including protection from unauthorized system administrators. It can be compared to a safe deposit box at a bank that protects an individual's valuable assets, even from bank employees.

Scalable base can be extended to support registration and certification across organizational boundaries. IBM Vault Registry integrates the vault software with a public key infrastructure to enable the implementation of multiple registration and certification authorities under consolidated systems and operations management.

In addition to the above benefits, Service Providers have the following reasons to Use IBM Vault Registry:

Strengthens client-provider trust. IBM Vault Registry provides a solution that strengthens the trust among clients and customers wanting to conduct e-business using the security provided by digital certificates, but were hesitant because of security and third-party trust concerns.

Offers new revenue opportunities. IBM Vault Registry offers the business potential of being a Certificate Authority to build trust into business-critical applications for clients over the Web.

==========

APPENDIX

I. References

For more information about Web security, refer to:

- Retooling Business for the Web, Understanding the Secure, Trusted Infrastructure for e-business at http: //www.software.ibm.com/ commerce/ registry/

For detailed information about Vault Registry, refer to:

- The IBM Vault Registry Information Guide, GH09-4516-00 in the Vault Registry Library at http: //www.software.ibm.com/ commerce/ registry/ library.html

II. Selected PKI definitions

The Public Key Infrastructure is a catchphrase for a range of evolving standards for security based on public key cryptography. The PKI is a system of digital certificates, certification authorities, registration authorities, certificate management services, and distributed directory services used to verify the identity and authority of parties involved in any transaction over the Internet.

The **Registration Authority (RA)** is the organization, processes, procedures, software and systems that actually approve, renew, suspend or revoke a Digital Certificate. The RA is responsible for validating that the recipient of the Digital Certificate (a person, application, server, hardware device, file, etc.) is authorized to perform the privileges associated with that Digital Certificate.

The **Registration Application** is the procedures, software and systems that enable the ultimate end users to register for a business process. The Registration Application enables the user to interact with the RA, and is the often the means by which the digital certificate, issued after RA approval, is returned to the user.

A **Certificate Authority (CA)** is the organization, processes, procedures, software and systems that control the issuance, renewal, suspension and revocation of a Digital Certificate. It may also be responsible for maintaining and publishing a list of the user community through an online directory.

A **Digital Signature** is a coded message added to a document or data that identifies the sender and also provides information integrity. A digital signature can provide a greater level of security than a physical signature.

A **Digital Certificate** is an electronic credential issued by a trusted third party to a person or entity. Each certificate is signed with the private key of the CA and vouches for an individual, business, or organizational identity.

The **Digital Certification** process occurs when a trusted third party, such as a CA, issues an electronic credential that vouches for an individual, business, or organizational identity.

Public / private key pairs provide the foundation for several security cornerstones including transaction privacy, information integrity and authentication. Each person gets a pair of keys, one called the public key (which is available publicly) and the other called the private key (which the user keeps secret).

Publishing of public keys. Any other user on the network uses your public key to encrypt messages for your eyes only. Public keys for each community member are published in an online directory.

III. Applications by Industry

Potential Business and Government Uses of IBM Vault Registry

The following list provides a number of examples that highlight the potential applications of registration and certification for individual sectors of business and government.

IBM Vault Registry would provide the platform for registration, certificate management, authentication, logging and electronic vault security. The customer or 3rd party developer would integrate PKI into existing applications or create new applications.

As digital certificate technology is accepted in the marketplace, thousands of additional applications will emerge, literally transforming the digital world and expanding the capabilities of the Internet.

Transportation-freight
Register shippers, recipients and customs agents; grant access to shipping records and shipment manifests; enable tracking of freight and container whereabouts.

Transportation-passenger (airline)
Register passengers, airline workers and security staff; control physical access to different parts of the transportation system; support certificate-based enrollment and records management for frequent flier and preferred customer groups; issue, accept and reconcile digital tickets

Postal organizations
Provide public registration and identification services. Provide electronic post office boxes, time stamps and archives. Support infrastructure security for package tracking and sensitive email.

Communications (telephone, cable)
Provide user authentication and access control for telephony, interactive television, service and customer security.

Utilities - Electric
Register employees and third-party energy brokers; control access to utilities' capacity and availability scheduling to facilitate trading of surplus power between utilities.

Wholesale Trade
Register businesses and their authorized representatives, banks and business brokers. Facilitate issuance of Letters of Credit, digital RFPS, and validation of orders.

Retail Banking
Register customers, employees and businesses to provide services through digital networks, such as home banking, credit/ debit card transactions, encrypted forms (loans and account applications), electronic-checking, funds transfers, electronic safe deposit boxes, etc.

Commercial (Merchant) Banking
Register trading partners to provide commercial services over the Internet such as commercial banking, encrypted forms (loans and account applications), electronic-checking, bill presentment and payment, funds transfers, electronic safe deposit boxes, etc.

Capital markets financial institutions (investment banking and securities trading)
Register, license and certify securities and commodities brokers, trading venues, securities issuers and registrars. Register clients and their financial institutions for Internet securities trading, payment and clearance. Provide online facilities to accept and maintain personal account information and brokerage analysis tools.

Health care industry, HMOs
Register, credential and certify physicians and provider institutions. Provide digital identification of physicians for on-line filing of patient records, billing, and remote treatment programs. Provide encrypted archives for patient and practitioner records, prescription rights. Support distributed professional collaboration.

Medical insurance
Register patients, insurance providers and third-party payors. Register insurance staff for case management and claims processing authority. Provide security-rich platforms and applications for case management, medical outcomes studies, claims processing, patient records, delivery of pharmaceuticals.

Insurance agents, brokers, and services
Register insureds: covered individuals, beneficiaries, insurance providers. Register brokers and third-party estimators for customer on-line filing (signing and time stamping) of applications and claims forms, access to rates, policy and account information. Register insurance staff and third-party assessors for loss estimation and claims processing authority.

Real estate
Register brokers and assessors. Authenticate buyers and sellers. Certify credentials for on-line property sales and listings. Certify property assessments. Provide electronic escrow (archive) for purchase and security deposits, and sales contracts.

ISPs and on-line services
Register online users and provide access control to proprietary Internet services, forums and content areas. Provide escrow security for service pre-payment deposits.

Software designers and companies
Register "gold" copies of software. Digitally sign software copies to establish integrity. Register end users for software licensing, support, service and upgrade contracts.

Entertainment industry
Register "gold" copies of videos and music albums. Digitally sign product to combat theft. Register users for purchasing clubs, user groups, promotions, etc.

Educational services
Register students and teachers. Provide facilities for on-line courses and registration for classes at universities. Provide electronic credentials for graduates and staff.

Membership organizations
Register members; provide digital credentials and certification of professional qualifications. Certify members rights and privileges for access by the world at large.

Governments
Register benefits recipients. Authenticate and certify entitlements (Social Security, Welfare, Medicaid, Medicare, Food Stamps, Assistance Programs). Provide facilities for personal identification and authentication, tax filing, benefit distribution, business certification, regulatory compliance.

Armed forces
Register recruits and staff. Authenticate and certify access rights, security clearances, etc.

Engineering, accounting and property management
Register professionals; provide digital credentials and certification of professional qualifications. Certify members rights and privileges for access by the world at large. Provide facilities for on-line tax filing, depositions, reports, and analysis.

Large corporate/ institutional intranet usage

Register critical applications (databases, transaction applications), users and privileges. Certify members rights and privileges for access by company systems.

Manufacturing
Register suppliers and provide certificate-based parts procurement, service management, sales management.

Enterprise Security
Register employees. Provide certificate-based single ID logon, encrypted email, virtual private networks and remote access to applications.

Large corporate/ institutional Internet usage
Register customers, clients, business partners, suppliers, employees, other stakeholders. Provide certificate-based access control to systems and applications. Support generic business needs including physical building access, HR applications (Personnel, Payroll, Expense Accounts, Benefits), ERP applications (Purchasing, BOM, Parts, Asset Management, etc.), financial systems (General Ledger, AP, AR), and business cycles such as procurement, warehousing, manufacturing, distribution, treasury, etc.

Networked Application Service Providers
Provide multiple customers with individually branded Certificate Authority (registration, certification, signing, PKI, public/ private keys, encryption, timestamping, notarization, certificate authentication, cross-certification, etc.)

IV. IBM Vault Registry Usage Scenario*

IBM Vault Registry can play a vital role in delivery of business and governmental services, delivering improved customer service, efficiency and security. The following scenario describes how Vault Registry would actually work for end users and system administrators. The particular steps and services will vary depending on the purpose of the application—see the Applications by Industry section for representative applications that can benefit from Vault Registry.

A service organization has created a Web-based e-business application. The organization could be an insurance, healthcare or financial services company or a government agency. The application will allow customers or clients to take more control over their account and relationship with the organization. Here are some of the end user features, benefits and advantages afforded by Vault Registry.

The Opportunity

- **For insurance**, policy holders can access all policy information through a self-service application. Questions and updates can be handled 24 hours a day. Using a Web browser, they can quickly enroll, update, manage their policies, and file claims (including digital evidence of loss). Agents and Brokers can check coverage and structure policies on behalf of clients. Claims assessors can report findings and file digital evidence (such as a digital photograph).

- **For healthcare**, medical provider organizations can manage records and submit insurance claims via a Web site. Insurers can process claims, arrange payment and handle all correspondence through the site. Patients can describe symptoms and treatment progress and check status of any claim at any time. Physicians can record medical findings and report on services delivered.

- **For financial services**, customers can view all their bills at one site and schedule payment. They can examine information about investment opportunities and change holdings at any time. Creditors can enjoy a dramatic drop in postage and paper document production costs. Creditors and financial institutions can reduce transaction costs through automating payment processing.

- **For government services**, citizens can check property and tax accounts, apply for licenses and entitlements and provide opinions from home. Employees can work through a single interface through a Web browser instead of several applications on different platforms.

The Problem

For service applications to be successful, they need to have a level of trust commensurate with the particular situation and its requirements for security and trust. All the users must be authenticated and verified. The data must remain private and integrity maintained. Security measures built into typical browsers, Web servers, and the firewall software do not deliver this level of trust.

Digital certificates along with other cryptographic technologies can create a highly trusted environment by providing access control, authentication, information integrity, transaction privacy and lower the likelihood of successful repudiation. A digital certificate is a form of credential that can be compared to a credential in the physical world such as a passport. It provides a means of identification from a trusted authority. For a digital certificate to be trusted by all parties, it needs to be issued in a way that makes it worthy of trust. For example, a passport dispensed by a vending machine has a lower level of trust compared to one issued by a recognized authority such as an embassy. Likewise, a digital certificate is only as trustworthy as the authority who issues it **and** the environment in which it is issued.

Most service organizations, whether private or public, would like to create and manage a registration and certification solution in house. The registration and certification process has to be flexible enough to allow for the organization's unique needs, such as its policies and standards and its affiliated organizations and service providers. **Some** of the issues that the sponsoring organization needs to address are:

- reducing the risk of fraud and security breaches associated with online applications
- maintaining the integrity and privacy of data and transactions protecting current IT investments
- deploying new technologies while controlling cost and complexity
- growing with future operational needs
- supporting the implementation after deployment

The Solution

The solution is **IBM Vault Registry.** IBM Vault Registry is a digital certification solution which provides integration of a Registration Authority, Registration Application, Certificate Authority, and an X. 500 directory, combined with innovative vault software, to enable trusted applications. It implements an enhanced trust model that reduces the risk of compromise to the integrity, authenticity, and information privacy of Web-based applications. IBM Vault Registry provides a

scalable solution that is designed to assist service organizations in meeting their growing needs to provide security-rich Internet access to their customers, employees, service affiliates and other stakeholders.

IBM, a leader in e-business and security solutions, backs the solution with service, support, education, and training from both IBM and IBM Business Partners around the world.

How the registration process works:

The registration approval and certification issuance processes are transparent to the user and require nothing more than filling out an on-line form and retrieving the certificate.

Users access the customer service Web site over the Internet. From the customer service Web page, the customer can select the registration option and complete the registration form. The form requires several pieces of sensitive and personal information, presumably known only to the user. After the form is completed, it is submitted to the organization for review and approval. The application form information is sent encrypted using SSL technology supported by the Internet browser before it is sent over the Internet to the service organization.

At the service organization, the completed form is passed to the registration application, built into IBM Vault Registry. There, the form is checked for completion (either automatically or manually) and the information is compared to a set of rules defined by the organization. For example, a rule may require that an applicant provide one of several kinds of documentation attesting to their identity before enrolling for services or entitlements.

To maintain a trusted and protected environment, all data is encrypted and stored in *vaults* -- special areas of memory which can be accessed only after the proper identification is presented.

Each certificate applicant is assigned his or her own vault. The information stored in a vault is accessible only by the owner of the vault or anyone authorized to access this vault. This provides an enhanced level of data privacy and integrity. Moreover, data communicated between vaults is encrypted and signed, providing an additional level of security against tampering.

When the registration application is approved by the Registration Authority, a request is sent to the CA to issue a new certificate. The certificate is generated and sent to the customer's personal vault, and the certificate information is published on the publicly accessible repository (the X. 500 directory). The user can now access his/her personal vault and download the digital certificate into their browser.

Using the digital certificate

The registered user can now access the organization's Web site and select the appropriate service options. He or she is prompted to present the digital certificate. The digital certificate is an electronic credential issued by the organization which allows access to the applications over the Internet. The user clicks on the certificate stored in their browser and it is sent to the service application.

The service application can either use the Vault Certificate Validator to check the validity of the certificate or perform its own checks. If the Validator is used, it checks against the X.500 directory and the certificate revocation list (CRL) to make sure the certificate has not been revoked.

Solution Benefits - Why IBM Vault Registry?

The benefits of using the IBM Vault Registry solution for enabling the service applications include:

- Encrypted registration process helps ensure that digital certificates are worthy of trust.
- Innovative "vault" software helps protect data and applications from disclosure to unauthorized users, including system administrators.
- Flexible approach enables integration with existing applications and customization for unique operational policies.
- Scalable base can be extended to support registration and certification across organizational boundaries.

IBM Vault Registry enables a seamless integration of the components needed by customers wishing to run their own Certification Authority, reducing the cost and complexity of assembling such a system from multiple vendor offerings. The IBM Vault Registry solution allows seamless integration of all major components for issuing and maintaining certificates, the registration process, and publishing certificate information and Certificate Revocation Lists in an X.500 directory.

*The scenarios described are applications that organizations can write and run on many application servers. The Webserver platform used by Vault Registry is one option. The certificates issued by the Vault Registry Vault Registration Application, however, can be used successfully with other applications.