White paper

Implications of digital certificates on trusted e-business.

e-business

Abstract: To remain ahead of e-business competition, companies must first transform traditional business processes using security technologies. They need to ensure the high levels of trust necessary to conduct secure online transactions with confidence. This paper describes the aspects of trust and security needed to enable successful e-business.

e-business is about transforming key business processes using Internet technologies—enabling companies to expand their presence into the vast global marketplace. Successful e-business is not only about transforming current business processes but exploiting new electronic commerce (e-commerce) opportunities before the competition.

By capitalizing on new market opportunities offered through the Internet, companies can realize the full potential of e-business and gain a competitive edge. For example, a bank could expand its limited online services—making all of the services available through its branch offices accessible to customers over the Internet. In addition to offering customers a more complete range of online services, this bank could also enable various businesses to post monthly billing information for bank customers. Ultimately, the bank would benefit from revenue gained by establishing profitable business-to business relationships that generate greater customer satisfaction, which, in turn, could lead to increased customer loyalty.

A successful e-business strategy can also increase the overall efficiency of business processes. For example, healthcare institutions could make online services available to doctors, patients and various medical service suppliers. This would not only reduce the time and costs associated with paper-oriented operations but increase efficiency through more timely and accurate delivery of information. Similarly, manufacturing companies could share important supply chain, inventory or design information through extranets, making information available to trading partners in a fast and efficient manner, reducing turnaround times and driving down carrying costs.

e-business enables companies to take advantage of emerging e-commerce market opportunities and to achieve greater overall business benefits, including:

- Increased revenue resulting from greater market penetration and reduced marketing costs
- Increased customer loyalty resulting from greater customer satisfaction
- Improved productivity and efficiency resulting from electronic processes and faster transaction times

Business considerations that inhibit e-business

The primary inhibitors to widespread adoption of e-business are security and trust. Traditional business practices allow transacting parties to establish trust through various means, including face-to-face contact. However, conventional means of authentication are not available for users of public, untrusted networks, such as the Internet. Password and personal identification number (PIN) security schemes do not adequately address this issue for the rigors of e-business.

While today's market is flooded with various security solutions that claim to address e-business needs, the cost and complexity involved in establishing, maintaining and protecting the levels of trust necessary for online business are prohibitive to most companies. The time and expense required to install, configure, integrate and manage numerous proprietary technologies from multiple vendors can delay deployment of e-business applications. The end result of this complicated endeavor must adequately address the risks of fraud and security breaches associated with online applications while providing users with the level of trust desired. The cost of security is not only limited to the monetary expense of products and systems operations but also includes the immeasurable damage caused by compromises to data integrity and transaction privacy. The resulting loss of trust can negatively impact customer relations and diminish a company's reputation.

To reduce the cost and complexity of deploying new technologies, companies need a security solution that integrates into the existing framework and leverages current IT investments. The solution should reduce the complexity of implementing and maintaining the security infrastructure so companies can concentrate their resources and time on growing their businesses.

Invest in trusted e-business

To succeed in e-business, companies must employ security solutions that protect against unauthorized access to business-critical transactions, data and services. Employees, business partners and customers should be confident they are being provided with the privacy and security required to safeguard sensitive information and network resources. At the same time, companies should be able to enforce their policies and business rules for business transactions efficiently.

To make trusted e-business possible, companies require integrated, policy-based security technologies that provide the same level of trust for online processes and e-business transactions as found in traditional processes, including:

- Authentication to check the identity of participants in an electronic transaction
- Access control to help prevent unauthorized users from gaining access to applications or data
- Transaction privacy to help prevent unauthorized users from viewing or reading sensitive information
- Data integrity to help protect against tampering
- Unique data trail to protect against loss resulting from fraud and to reduce the risk of transaction repudiation

Reducing the risk of unauthorized access

To meet the demand for online access to information while controlling access privileges to sensitive data, companies often rely on passwords and PINs. Passwords and PINs can provide adequate access control within a closed loop system, but they can be easily compromised. Neither PINs nor passwords provide sufficient security for users accessing applications through public untrusted networks.

Until companies can achieve the highest level of trust provided by their security solutions, the benefits of network computing are limited to running moderately sensitive applications or offering only partial services to customers. Because the Internet is an open, untrusted medium, a higher level of information integrity and authentication is required to limit or contain the risks of repudiation, data compromise and fraud. By implementing a policy-based security solution using digital certificate technologies, companies can define and enforce the unique security requirements across organizational boundaries and beyond—enabling a more secure and trusted environment for highly sensitive e-business transactions.

Digital certificates and public key infrastructure

A flexible and integrated security solution using digital certificates can help companies maintain the advantage necessary to enable e-business applications. By incorporating digital certificate technologies into the existing infrastructure, companies can establish, maintain and protect trust in a global, networked environment and extend their business applications across the Web.

Digital security technologies using public key infrastructure (PKI)—an evolving and widely accepted security standard based on encryption—can enable companies to define and enforce security policies, issue certificates and provide communication security. Security solutions using PKI for highly sensitive applications should offer a variety of services, including:

- Registration of users in a secure environment so that credentials can be trusted
- Management and control of the registration process according to company policies
- Integration to back-end systems' existing databases to accommodate automatic verification of registration data
- Protection against unauthorized, third-party interception of transaction and information, including internal staff
- Audit trail of transactions
- Storage of business-critical information and user data in encrypted, online repositories
- Ease of implementation and management by integrating all key components to enable security and trust in applications
- Scalability to grow with business needs

The result is a solution that is easy to implement and manage, allowing companies to concentrate on business application development and enabling them to stay competitive in the marketplace.

To realize these benefits, companies need a security solution that can provide a registration authority, a certificate authority and a repository for data storage. This solution would allow companies to reap the benefits of Web-based business instead of spending time and money building comparable solutions from multiple vendor offerings.

Establish, maintain and protect trust

To maintain and protect a trust relationship between the user and the company, it is vital that electronic registration use strong technological and procedural safeguards based on clearly defined procedures and strict evaluation criteria. The registration process is key to establishing trust from the very beginning so that the end result of this process, the issuance of a digital certificate, is trusted.

The registration process allows users to apply for digital credentials from a registrar or registration authority (RA), providing them with access to services offered by the company. The organization enforces its policies through the RA that makes the decisions about certificate approval. The RA evaluates the data provided during registration to determine the applicant's eligibility for a digital certificate. If approved, the RA requests the certificate authority (CA), a trusted third party, to issue the certificate to the applicant.

The CA handles the technical and administrative tasks of issuing and managing certificates. The CA issues a certificate, which essentially vouches for the holder's authenticity in accordance with the CA's defined limits and policies. The CA may also be responsible for maintaining the certificate directory where certificate information is logged and stored.

The level of trust and intrinsic value of the digital certificate is only as good as the environment and process through which it is issued. The nature of the registration process will, in effect, dictate the level of trust in the certificate issued—the more secure the registration environment and the strict adherence to company policies, the greater the inherent value of the certificate. The level of trust and value in a certificate could be compared to that placed in a passport issued by an embassy versus an identification card offered by a department store.

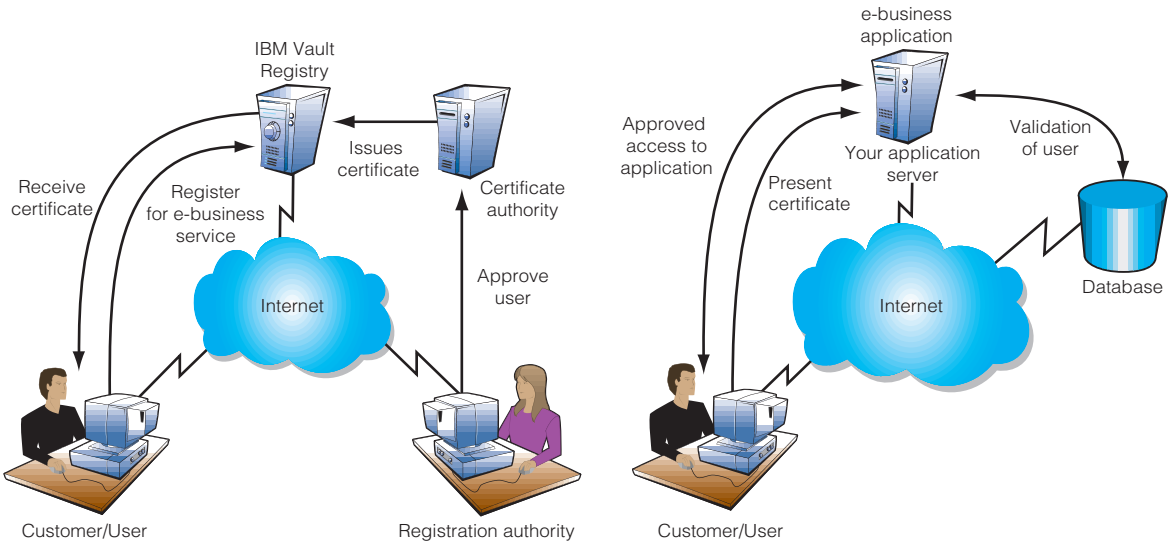
To enforce accountability, there are procedures underlying the certification process that isolate specific duties, authority and privileges. The certificate must be verifiable and recognizable as a reliable, trustworthy and effective mechanism. This requires the systems that publish and verify certificates to support inquiry over the Internet or private networks. It also requires revocation and expiration of an issued certificate to be promptly logged so that security breaches can be reduced.

Digital certificate technologies using PKI make it easy for companies to employ the advanced security measures necessary to ensure trusted e-business.

IBM Vault Registry

IBM® Vault Registry, IBM's integrated registration and certificate solution, addresses customers' security concerns associated with conducting business over the Internet. Vault Registry responds to the business requirement for improved security of the registration and certification process by protecting sensitive personal information. Vault Registry's extended trust model greatly improves authentication, privacy and reduces the risk of repudiation among transacting parties by shielding sensitive documents, services and business applications from internal and external breaches.

Vault Registry provides a trusted environment for registration, using encrypted electronic *vaults* to help protect data from unauthorized access and fraudulent authorization of applications. By integrating the key components needed to apply, issue and manage digital certificates, Vault Registry reduces the overall complexity and cost involved in implementing and managing the certification process.



Registration and certification
Web-based administration and distribution
All data transfers and storage are secured using encryption

Your e-business application
User access to application

IBM Vault Registry registration process

IBM Vault Registry allows companies to:

- Register customers, employees and authorized representatives for services offered through digital networks with security
- Issue, manage and maintain certificates to authenticate users accessing a company's services
- Integrate with existing back-end databases to support automatic verification of registration data through flexible policy exits
- PKI-enable applications using certificates to grant access, maintain transaction privacy, protect data integrity, provide authentication and reduce the risk of repudiation
- Maintain audit records of transactions
- Employ vault facilities to help protect against unauthorized access to sensitive data or applications, even by internal systems administrators

IBM Vault Registry offers the flexibility and scalability needed to address real e-business requirements, providing integration with existing databases and customization of the registration process according to particular business policies. Its high performance and serviceability include support for robust, high-availability operations, as well as tools and procedures that address system-wide recovery and integrity in the event of failures. While Secure Sockets Layer (SSL) encryption protects data during transit, Vault Registry provides a complete solution by extending data and transaction security to the server.

Part of the total IBM integrated security solution

IBM Vault Registry is a component of IBM SecureWay® FirstSecure, delivering comprehensive security solutions that enable e-business. IBM Vault Registry can be purchased separately or as part of SecureWay FirstSecure.

For more information

For more information about IBM Vault Registry, visit our Web site at:
www.ibm.com/software/security/registry

IBM Corporation
Department VK4A
3039 Cornwallis Road
Research Triangle Park, NC 27709

Produced in the United States of America
5-99