Building trusted e-business with Public Key Infrastructure

Although e-business uses a sophisticated technical foundation and continues to grow based on innovative technology, its ultimate success relies on a very human sentiment—trust.

Trust enhances all relationships—personal, professional and commercial. For participants in a relationship to trust one another, they must be sure of several factors:

- Who they are dealing with
- That transactions or conversations will remain private
- That information shared is true and reliable
- That the other party will not claim an interaction never occurred

In a networked world, in which interactions occur without physical contact, trust becomes paramount. Reducing levels of trust are the facts that transactions lack personal interaction, transactions occur in an untrusted environment, and there is risk of information interception and tampering.

Hence, for businesses and individuals to be comfortable with electronic transactions, they must establish, maintain, and protect trusted relationships. Ironically, creating an environment that supports this very human sentiment requires that the e-business infrastructure support trust mechanisms based on some very sophisticated, though easily implemented, technologies.

Organizations can create a trusted environment for e-business by using Public Key Infrastructure (PKI) technology, which encompasses standards-based trust mechanisms along with a certificate policy specifying roles, responsibilities, and privileges.

The Role of PKI in a trusted e-business

The role of the PKI is to provide the technological foundation for trusted e-commerce. PKI capabilities help create and manage credentials, certificates, and cryptographic keys required by applications. A critical advantage of PKI over predecessor cryptographic technologies is that end users potentially need to keep track of only one secret, their private key, as opposed to multiple shared secret keys, depending on the number of communicating parties. With PKI, technologies such as encryption, digital signatures, authentication, and directories work together to provide a comprehensive security infrastructure.

The following key PKI components provide the capabilities to establish, maintain and protect trusted relationships.

The **Certification Authority** (CA) creates and signs digital credentials (called *Digital Certificates*), maintains lists of revoked credentials (certificate revocation lists [CRLS]), publishes certificates and CRLS for the community of interest, and provides a management

interface for certificates and CRLs. The certificates allow applications to identify users and also allow easy exchange of keys used to facilitate privacy. The CA should be operated under strict security procedures and its actions audited.

The **Registration Authorit**y (RA) evaluates the credentials and relevant evidence that a person requesting a certificate is as claimed, vouches for the association of an individual with his electronic identification and public key (to the extent identified in its Certificate Policy or Certificate Practice Statement), and approves the request for issuance of a certificate by a CA. The RA acts as an interface between the CA and individuals requesting certtificate services. These services include request for renewal of certificates that have expired and requesting revocation of certificates. A revocation request may be due to a change in the status of the individual or change in the status of the individual's private key.

The RA consists of personnel, procedures, software, and systems that allow people or devices to register to use a particular business system. For example, a bank may require an applicant for Internet fund transfers to fill out an on-line form to verify the applicant's qualifications. If the requester meets the security and business requirements, the RA will approve the application and a digital certificate will be issued by the CA.

A **Public/Private key pair** along with cryptographic algorithms is used to encrypt documents, sign documents and identify people and verify whether documents have been modified. The private part of the key pair should be protected by the individual who it is issued to, while the public part of the key pair is widely distributed to others. Functions performed by one part of the key pair can be validated only by using the other part of the key pair. For example, a document encrypted by the public key can only be decrypted by the private key, which depending on encryption strength, may be virtually impossible to duplicate.

Digital Certificates bind a person's or device's identity to his public key and is issued by the Certification Authority (CA). Digital certificates enable Internet applications and other users to identify the person or device on the other end of a transaction. Just as someone might use a passport as identification when cashing a traveler's check, an application can use a digital certificate as identification when performing a transaction.. Although the digital certificate serves as identification, it is only as trustworthy as the organization and systems that issue the certificate.

A Digital Signature is a block of data created by applying a cryptographic signing algorithm to some data using the signer's private key Digital Signatures may be used to help message recipients determine whether anyone has tampered with a message since the time it was sent by the signer and to identify the source of the message.

The graphic from the long paper PKI Enables Trust Across the Extended Enterprise' needs to be added here.

Establishing, maintaining, and protecting trust

Having a secure, well-defined registration process is critical to ***establishing*** trust. Any vulnerability in this process can lead to weaknesses throughout the PKI implementation. Registration takes many forms, but generally, applicants who want a service or some specific privilege or entitlement apply to a Registrar or RA. For the process to be trustworthy, registration should be performed according to defined procedures using strict evaluation criteria. Furthermore, registration requires technological and procedural safeguards.

When a requester submits an application, the RA checks the veracity of the information with available document sources or trusted third-parties familiar with the applicant to the extent the RA deems necessary. The RA also evaluates the submission to help ensure that it meets the requirements, policies, and guidelines it has adopted for certification.

Once approved, the application is sent to an affiliated CA. Based on the RA's approval, the CA will, for a defined period of time, "vouch" for the applicant's certification for a certain level or for a defined purpose 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.

A certificate provides a means for establishing trust for a finite interval or period of time. To ***maintain*** trust after the end of that interval, users can apply to renew their certifications. The RA again reviews the application and instructs the CA to renewed or reissue the certificate. As before, the CA sends the new certificate to the applicant and publishes it in a repository or directory. If the trust is ever determined to be broken, the certification can be revoked.

Underpinning the registration and certificate management processes, there must be a robust technology infrastructure that helps ***protect*** the RA's work-in-process, registration records, and approval mechanism and the CA's certificate signing mechanisms and records. Ideally, this infrastructure employs security procedures that isolate each registration role and work process, so that registration itself is shielded from technological or human assault.

Overall, a trusted e-business relies on PKI to operate in accordance with a Certificate Policy and Certificate Practices Statement to perform the following services:

- Register users, users are people engaged in e-business activities and they are also the transaction applications that make those e-business activities possible,
- Issue certificates, publishing them in a directory accessable to the community of interest
- Renew certificates and revoke them as necessary
- Support applications that use certificates to grant access, maintain transaction privacy, help ensure information integrity, perform authentication, and address non-repudiation issues,
- Audit records to confirm completed transactions and detect tampering attempts
- Archive data and in-process transactions in physical or logical facilities that help protect against repudiation

In turn, these services allow an e-business to:

- Protect transactions, even when they flow through untrusted, third-party intermediaries
- Maintain auditable records of important transactions

- Hold business-critical information in encrypted, online repositories

An e-business enabled through PKI has all the capabilities needed for building trust relationships with customers, employees, business partners, and suppliers. Without PKI, an e-business is more exposed to data tampering, invasion of privacy, repudiation, and theft.

Implementation considerations

Several important factors can have an impact on the effectiveness and the cost of a PKI implementation if they are not considered beforehand. By its very nature, e-business requires that PKI solutions interoperate with applications and users outside the company. Therefore, PKI implementations and the entire security foundation should be based on recognized industry *standards* to promote interoperability**.**

A PKI implementation also needs to be *scalable* to provide services for the expected quantity of users—even up to millions of users. To lower total cost of ownership, it should allow multiple registration authorities under consolidated systems and operations management. Scalability is also critical for the support of certification across organizational boundaries. Finally, scalability involves not only the ability to support millions of users, but also the ability to support them cost effectively by automating most of the certificate management functions.

Companies wishing to operate their own PKI will benefit greatly from an *integrated* solution, where the components work together seamlessly. An integrated solution can reduce the cost and complexity of assembling a system from multiple vendors. Furthermore, companies will need to integrate their PKI solutions with existing backend systems to protect and leverage existing information-technology (IT) investments.

It is also important to be *flexible*. Flexibility provides investment protection to meet future application requirements for certificate validation. In a simple case, a Web server can validate a certificate by checking the expiration date and then verifying that the certificate was signed by a trusted CA . In many other cases, the server would also need to access a CRL to ensure that the certificate has not been revoked. In still other circumstances, the application may look at a directory, authorization table, or ACL to verify the specific privileges of the owner of the certificate.

Furthermore, the registration process, which serves as the entry point into the e-business, must be flexible to accommodate a company's policies and requirements. Without this type of flexibility, an organization would find it difficult to incorporate its business practices in the PKI implementation and ensure that its certificates can be trusted.

PKI implemented with IBM SecureWay Trust Authority

The thought of implementing any kind of infrastructure—public key or otherwise—brings to mind images of destroying the existing IT foundation, which is a chilling thought for any IT organization. IBM SecureWay® Trust Authority is specifically designed to integrate with backend systems, thereby protecting and leveraging the systems already in place.

Trust Authority runs on IBM AIX/6000® and Microsoft Windows NT® server platforms. It includes the following key features:

- A trusted CA manages the complete life cycle of digital certification. To vouch for the authenticity of a certificate, the CA digitally signs each certificate. It also signs CRLs to vouch for the fact that a certificate is no longer valid. To further protect its signing key, you can use cryptographic hardware, such as the IBM SecureWay 4758 PCI Cryptographic Coprocessor with the AIX/RS6000 server.
- An RA handles the administrative tasks behind user registration. The RA should be used to help ensure that only certificates that support a company's business activities are issued, and that they are issued only to authorized users. The administrative tasks can be handled through automated processes or human decision-making.
- A Web-based enrollment interface makes it easy to obtain certificates for browsers, servers, and other purposes, such as virtual private network (VPN) devices, smart cards, and secure e-mail.
- The Trust Authority Client, which runs under Windows, enables end users to obtain and manage certificates without using a Web browser. A Web-based administration interface, the RA Desktop, enables authorized registrars (Administrators) to approve or reject enrollment requests and administer certificates after they have been issued.
- An Audit subsystem maintains audit records, encrypted for security, for all important transactions. It computes a message authentication code (MAC) for each audit record. If audit data is altered or deleted after it has been written to the audit database, the MAC enables you to detect the intrusion. Audit records may also be signed when archived.
- Policy exits enable application developers to customize the registration processes according to a company's defined policies and procedures.
- Integrated support for IBM SecureWay Directory. The Directory stores certificates and revoked certificate lists in an LDAP-compliant format.
- Standards-based interfaces, including:
  - IETF PKIX Certificate and CRL Profile (RFC 2459)
  - IETF PKIX Certificate Management Protocols (RFC 2510)
  - IETF PKIX Certificate Request Message Format (RFC 2511)
  - IETF PKIX Operational Protocols - LDAPv2 (RFC 2559)
  - IETF PKIX LDAPv2 Schema (RFC 2587)
  - ITU X.509 V3 Certificates
  - PKCS#10; PKCS#7; PKCS #11

- LDAP V3
- RSA, DSA MD5, and SHA-1 cryptographic algorithms

IBM SecureWay Trust Authority solution components

Trust Authority components include:

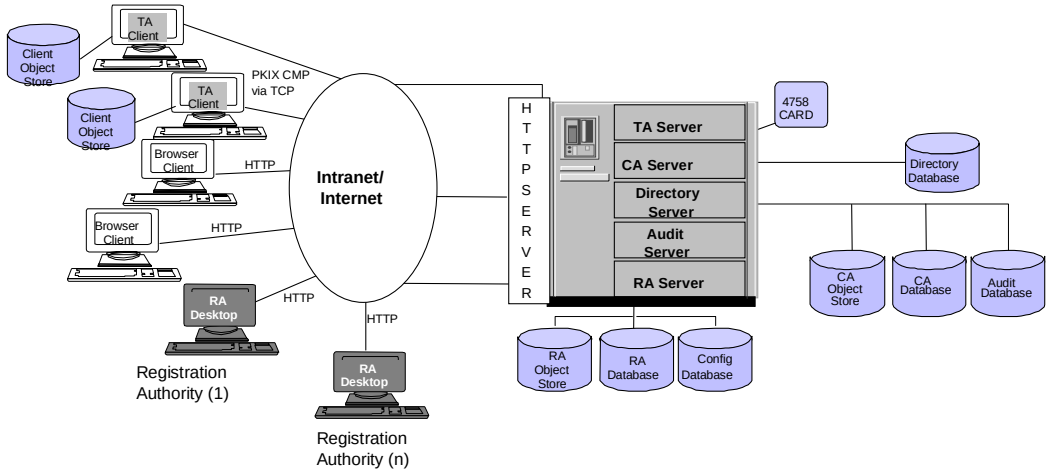
- Trust Authority server
- Registration Authority server
- Certificate Authority server
- Audit server
- Web server
- Database server
- 4758 Cryptographic Coprocessor (optional)
- Trust Authority Client

Exhibit 1 depicts a Trust Authority configuration in which the server programs coexist on a single machine. The server programs may be distributed among multiple machines. for load sharing or security considerations. The specific configuration depends on the desired levels of responsiveness, availability, and robustness.

Exhibit 1 Trust Authority components on a single platform

Trust Authority server

The Trust Authority server is the central server that ties the other components together. It maintains the configuration database and provides utilities for administering the system.



Registration Authority server

The Registration Authority (RA) is the server component that manages the registration process. It can be used to help enforce local business policies to provide heightened confidence that certificates are issued only to approved entities for approved purposes. The primary tasks for an RA include:

- Confirming the identity of the requesting party (to the level and through the methods chosen by the user)
- Verifying that the applicant is entitled to a certificate containing the requested or authorized attributes and permissions
- Approving and rejecting requests to create, renew, or revoke certificates
- Verifying that a party requesting a certificate holds the corresponding private key

- Enforcing the business policies, certificate policies, and resources in accordance with the organization's certification practices. In Trust Authority, the RA provides the framework to support a wide range of registration activities. When Trust Authority is configured, a registration domain can be used to enforce the policies. .

Enrollment

The RA provides support for a variety of enrollment protocols and certificate types. Enrollment features include:

- Use of a DB2 database to log encrypted registration and certificate data.
- Support for manual and automated registration and certificate request, renewal, and revocation approval processes.
- A collection of Java-based enrollment forms that allow users to request and obtain certificates using Web browsers. The enrollment process can be used to authenticate the client and server identities and deliver certificates to approved entities, with end-to-end encryption of all requested data. This process includes:
  - The delivery of certificates through the Secure Sockets Layer (SSL) for use with applications that are accessed from a Web browser or Web server
  - The delivery of certificates through the Public Key Infrastructure (X.509) (PKIX) Certificate Management Protocol (CMP) for use in a PKIX client application or to store on smart cards
  - The delivery of certificates that support the Internet Protocol Security (IPSec) standard for use with VPN applications or IPSec-enabled devices
  - The delivery of certificates that support Secure Multipurpose Internet Mail Extensions (S/MIME), for use with secure e-mail applications
  - The delivery of notification letters that inform applicants about the approval or rejection of a requestA collection of certificate profiles that make it easy for users to obtain the type of certificate they need. The profiles define the intended purpose of the certificate and the certificate's validity period. Based on information in the template, the RA is able to deliver a certificate in the proper format with the necessary certificate content.
- Support for pre-registration, a process that enables one user, typically an administrator, to request a PKIX-compliant certificate for another user. Using the Trust Authority Client application or other PKIX-compliant client, the end user can easily obtain the approved certificate without having to be knowledgeable about the enrollment process.
- Support for policy exits, which enables organizations to integrate customized steps in the registration process (such as accessing a corporate database to verify certificate eligibility during the enrollment process or adding a

user-defined extension to create an attribute certificate.) The RA includes a sample policy exit that performs automated approval processing.

The Java-based enrollment forms and certificate profiles serve as examples for customizing the enrollment process to meet specific, customer, certificate policies.

Administration

The Registration Authority Desktop (RA Desktop) applet allows authorized administrators to review applications for certificates, approve or reject requests, renew certificates, and revoke certificates. It supports such tasks as:

- Retrieving pending enrollment requests
- Querying the registration database to retrieve and act on records that match certain criteria
- Reviewing detailed information about a certificate or a request, such as the history of all actions taken since a request was first submitted
- Setting the validity period of a certificate
- Annotating a record to explain the reason for an action

The RA Desktop is a secure application that requires installation of some components on the Registrar's system. Only authorized RA Administrators can access the RA Server, which requires a valid digital certificate.. The RA Desktop and the RA Server communicate by using SSL at up to 128-bit encryption. Trust Authority provides a tool to add any number of RA Administrators to support the registration workload. When an Administrator is added, the registration domain is identified and Administrator's privileges are specified. For example, one RA Administrator may be allowed to approve and reject requests only, but another RA Administrator may be allowed to revoke certificates as well.

Customization

A registration application is provided with Trust Authority and may be used out of the box. However, many enrollment forms or registration processes can be modified to reflect specific organizational certificate polices and goals. For example, it may be desirable to display a corporate logo and special instructions on the browser enrollment form. Also the certificate profiles might be be changed to define extensions relevant to the class of users, servers or devices planned for enrollment.

After installation and configuration of Trust Authority, many of the files that define the registration domain can be copied and customized for specific business purposes. The following application files can be copied or revised. During configuration, these files are created in the directory path established for the registration domain.

- The configuration files (file type .cfg) installed in the /etc subdirectory. For example, use these files to adjust a runtime setting for the RA server or RA Desktop.

- The sample notification letters (file type .ltr) installed in the /etc subdirectory. Trust Authority provides sample text to inform users when a request has been approved or rejected. These samples can be customized or replaced, as desired.
- The HTML (file type .html), graphics (file type .gif), and Java Server Pages (file type .jsp) installed in the */webpages* subdirectory. For example, you may want to alter the text and graphics displayed in the browser enrollment forms. An existing certificate profile can be customized or a new one defined to support the organization's certificate policies.
- The policy exit (policy_exit) installed in the /bin subdirectory. Trust Authority provides this exit as an example of how to handle automated approval processing. Other exits can be written to integrate registration processing with other applications or to process specific, organizational, registration actions.

Certificate Authority Server

The Certificate Authority (CA) is the server component that can be used to manage the certification process. The operator of the CA acts as a trusted third party to help promote trust between users who engage in e-business with each other. It vouches for the identity of certificate users through the certificates it issues. In addition to identifying the user, the certificate includes the user's public key, which can be used for several e-business transactions.

In such a security model, the trustworthiness of the parties depends on the trust that is placed in the CA that issued the certificate. To help provide for the integrity of a certificate, the CA digitally signs the certificate as part of creating it. Attempts to alter a certificate will invalidate the signature and render it unusable.

The CA provides transaction environment security in the following ways:

- To help ensure the uniqueness of a certificate, the CA generates a serial number for each new certificate and for each renewed certificate. This serial number is a unique identifier and is not stored as part of the distinguished name (DN) in the certificate.
- To track the certificates it issues, the CA maintains an issued certificate list (ICL). The ICL stores an encrypted copy of each certificate, indexed by serial number, in a DB2 database.
- To track revoked certificates, the CA creates and updates CRLs. The CA and RA exchange messages as soon as the revocation occurs, which enables the CA to update the CRL immediately or during the next periodic update, depending on your CA policy. Just as it signs certificates, the CA digitally signs all CRLs to vouch for their integrity and authenticity. After signing, the updated CRL is published in the Directory.