IBM
Home | News | Products | Services | Solutions | About IBM
ShopIBM Support Download
Search Go
IBM : Security : Library : Papers

Securing IBM Applications with Public Key Infrastructure

This document is also available as a PDF file.

Businesses are becoming increasingly dependent upon the Internet for their most sensitive communication, as evidenced by the growth of extranets and electronic commerce. This dependence upon public electronic networks requires a standard security infrastructure capable of handling a wide variety of tasks in a consistent and unobtrusive manner. This document describes such an infrastructure and outlines its advantages for IBM, its customers and partners.

How Can You Trust Someone You Don't Know?

Trust is the cornerstone of secure communication over the Internet. How can you trust that the party on the other end of the wire is who they claim to be? How can you trust that a communication was not intercepted or changed before it reached you? Two examples serve to illustrate the issue of trust.

Online purchasers need a secure method of transmitting credit card information, but, more importantly, they need to know whom they are transmitting the information to.

While an SSL (Secure Sockets Layer) transmission of credit card information acts as a steel pipe to prevent tampering en route, it does not address the identity or trustworthiness of the individual at the other end of the pipe. Since a URL is no more difficult to obtain than a telephone number, telephone-based boiler room operations (that fraudulently obtain credit card data and then disappear) can easily move online.

Similarly, secure transmission of sensitive documents over extranets or through e-mail requires the ability to guarantee the confidentiality, authenticity and integrity of messages. The sender of an electronic message wants to be sure that only the intended recipient can read the message. The recipient wants to be sure that the message is truly from the sender. Both parties want to be sure that the message received is identical to the message sent.

Both of these examples point to the same problem: How can you trust someone you don't know?

Trust Management

The answer to the question, "How can you trust someone you don't know?" is that you can't, unless you know a trusted third party who can vouch for them. In electronic communication, this trusted third party is called a Certificate Authority (CA). The CA's job is to check an individual's credentials by demanding physical proof of identity. When the CA is satisfied with the individual's proof of identity, it issues a digital certificate. The US Post Office and VeriSign are both examples of Certificate Authorities. A significant policy aspect of trust management is deciding whether to accept the authority of a particular CA. Such decisions are based on reputation, information and experience.

Certificates and Keys

A certificate acts like a passport or letter of introduction, identifying an individual who travels the electronic highway. Like a letter of introduction, a certificate does not grant entry, it simply identifies an individual and provides a referral based on the reputation of the issuer. Like a passport, a certificate expires after a specified period of time and must be renewed regularly.

When a CA issues a certificate, it also binds a set of keys to the name on the certificate. These keys are used by the individual for electronically signing and encrypting communications. The value of a certificate is that it uses the backing of a CA to inextricably bind a known individual to a particular set of keys.

Public Key Cryptography

The keys bound to a certificate form the basis of Public Key Cryptography. Each key is a long string of numbers and letters. Keys are issued in pairs; one is public and the other private. The public key is advertised widely, while the private key is guarded as a secret.

Any document encrypted in an individual's private key can only be decrypted with their matching public key, thus guaranteeing the authenticity of a message. Encrypting a document with a private key is also called signing; if a valid timestamp is included, then encryption by the private key constitutes a digital signature that cannot be repudiated.

Similarly, any document encrypted in an individual's public key can only be decrypted using their corresponding private key, thus guaranteeing the confidentiality of a message.

Proof of a message's integrity is the by-product of its successful decryption.

Thus a message signed by the sender's private key and encrypted in the recipient's public key carries with it a guarantee of authenticity, confidentiality and integrity.

Requirements for Managing Trust

All of the above machinations are useless, however, without decent trust management. Yet trust management is a complex issue.

For example, if you're unsure of the CA's reputation, then you won't have confidence in the certificate. If you don't have confidence in the certificate, then you can't rely on the keys. If you can't rely on the keys, then you can't trust the digital signature and the whole system breaks down.

Trust management goes beyond the CA, however. It entails actions by the CA, the user and the software. The following guidelines can help manage the critical points where trust can break down:

The CA must require adequate proof of identity before it seals a name into a certificate.

- The CA must set forth and follow clear rules for repudiation and revocation of certificates.
- Certificates must expire before the amount of time elapses in which the certified keys could be reasonably compromised.
- Keys must be properly chosen, using both a strong random number generator and an adequate primality test, in order to prevent forged signatures.
- Prior to transferring keys to the owner, the keys' privacy must be carefully guarded.
- Key owners must protect their keys to keep them private.
- Key owners must not allow their private key to be applied without their knowledge or consent.
- Private keys to be used for signing documents (signature keys) should not be escrowed (sent to a third party or government agency) without careful consideration of potential consequences.
- Software must support the security of private keys, for example by prompting for a password before allowing a signature operation.
- Software must apply signature keys correctly and not confuse them with other kinds of keys.
- Software must support some a method of invalidating certificates, such as Certificate Revocation Lists (CRLs), in case private keys are compromised or a certificate is repudiated.

Trust management requires the CA to abide by their Certification Practice Statement, the user to keep private keys secret, and the software system to properly apply the rules of public key cryptography.

In addition, the software system must present to the user relevant information related to the use of keys and certificates in order to support the user's development of a security policy based on that information.

In the end, trust is the result of experience and information. Trust management must provide the user with

the tools required to make an informed trust decision.

The PKI Solution

The mechanisms, operations and policies described above are supported by a Public Key Infrastructure (PKI). A PKI provides a framework in which security services based on public key cryptography can be implemented in a distributed computing environment. The PKI provides for key management, certificate management, policy management, and repository access. Often, a PKI contains a high-level Application Program Interface (API) that handles tasks such as verifying and managing certificates, digitally signing documents, and managing keys. The API serves as a layer between application programs like secure e-mail and the underlying security protocols. The API allows applications to reliably use public key cryptography for security without being concerned about the details of its implementation.

The Internet Engineering Task Force (IETF) has proposed a draft standard PKI, called PKIX, that IBM is committed to supporting. PKIX is an open standard, meaning that it is platform-independent.

Existing PKI Implementations

Several companies have already implemented or announced various approaches to PKI.

Entrust

Entrust is a Canadian company that has developed and marketed a proprietary PKI that holds a large market share. Entrust has announced future support for PKIX interoperability, but its products do not currently support the standard. The Canadian government has decided to use Entrust as the basis of their federal PKI. This means that all software used by the Canadian Government must be Entrust compliant, which has given a large boost to the company and its technology. Entrust also licenses its technology to other companies.

Entrust is actively participating in the IETF PKIX effort, particularly in the arena of administration tools, where they have proposed that their approach be implemented as a standard.

Microsoft

According to Microsoft® WindowsNT® Distributed Security Services: Secure Networking using WindowsNT Server Distributed Services Technology Preview (© 1996, Microsoft Corporation), “The next version of WindowsNT security will use Internet standards for public-key security with features built into the operating system.”

Microsoft Windows NT 5.0 has announced support for both Kerberos 5 (a shared-secret security protocol) and public-key based security. While Kerberos will serve as the basis for NT security, external users will be given access to NT services via a certificate if the CA behind the user’s certificate is a “trusted CA.” NT will then assign access control rights based on an association between information in the certificate and some existing NT user account.

The Windows NT Certificate Server can be used to issue certificates to partners who need access to specific information resources, instead of setting up a user account or using NT domain trust. Public key cryptography is also supported in NT for the purpose of encrypting communications.

The Microsoft CryptoAPI 1.0 and CryptoAPI 2.0 libraries serve as the underlying cryptographic API in this implementation. There is no formal PKI in NT; instead, support for public key cryptography is built into the operating system. CryptoAPI 2.0 is also included in Internet Explorer 4.0.

Microsoft is also using public key cryptography in its AuthentiCode technology. AuthentiCode is basically Microsoft’s support for signed Java applets, called JARs (Java Archives). In a JAR, a certified developer digitally signs an applet using public key cryptography. The JAR serves as both a digital label and shrink-wrap, ensuring that the applet is not malicious.

Netscape

Netscape Certificate Server issues and manages employee certificates that can be used within an enterprise for digital signatures, message encryption, and single sign-on. Netscape also provides support for JARs through their Object Signing technology, which is analogous to Microsoft's AuthentiCode.

RSA

RSA Laboratories controls the patents on much of the technology in common use in public key cryptography. They also offer a product called Certificate Security Suite, which is a set of components for building applications that incorporate certificate security, making it easier for developers to build and integrate applications that rely on PKI.

Thawte

Thawte is a South African based CA. In addition to issuing various types of certificates, Thawte offers a Chained Certificate Authority Program which allows an organization to issue digital certificates to its own employees or members, and have those digital certificates recognized and trusted by all the software that trusts Thawte. Subscribers to the service manage their own certificate infrastructure, which is in turn certified by Thawte. Without chained certificates, such organizations would need to modify every browser and e-mail client used by their employees to recognize and trust their own certificate system. Thawte claims that the chaining process is secure, and that chained CAs are technologically and contractually limited to issuing certificates to their own members or employees.

Thawte also has a technology called Strong Extranet that allows institutions to encode customer information in the extensions to their customer's certificates. Because multiple institutions can add information, the user needs only one certificate, making renewal and revocation simpler, although the issue of modifying an extension to an existing certificate is not addressed.

Xcert

Xcert is a security infrastructure company whose Universal Database API (XUDA) is a proprietary PKI that claims to provide full, standards based cross-authentication. According to their Web site, "As one of the authors of the PKIX standards, we are committed to following the standards contained within the draft."

XUDA also provides a template system whereby a System Administrator can create Web-based applications that use certificates for authentication and access control simply by editing HTML files.

VeriSign

VeriSign is a CA that is a spin-off of RSA. In addition to acting as a CA, VeriSign offers three PKI options. VeriSign will provide companies software for an internal CA, outsource the entire internal CA operation, or outsource the backend processing for an internal CA. It is not yet clear, however, that companies, and particularly their MIS groups, will be willing to rely on an external third party to outsource such a sensitive component of their network security.

The SET Initiative

The Secure Electronic Transactions (SET) standard is a protocol for communication between vendors and credit card issuers like Visa and MasterCard that enables online commerce. SET is designed intentionally not to interoperate with other protocols. Although based on public key cryptography, SET requires the use of SET CAs and SET certificates. Because SET is limited to a narrow usage domain, it does not present a general-purpose solution.

Lotus Notes and Domino

Lotus was one of the first companies to recognize the value of PKI, and it is one of the few to have implemented it on a large scale. Lotus Notes and Lotus Domino currently use a proprietary PKI based on RSA technology to support user and application security. Along with the adoption of other Internet standards like X.509 and SSL, which are available in the current versions of Domino and Notes, Lotus is leverage its success with scalable PKIs by becoming an early mover behind the PKIX effort, thereby bringing its considerable experience into the open arena.

The PKIX Solution

As mentioned above, PKIX is the proposed IETF public key cryptography standard. It currently has the status of Internet draft, which means that IETF working groups are putting the finishing touches on the proposals before they are put on the standards track. The PKIX standard has garnered broad interest in the industry. Companies that are actively participating in the development of the standard include IBM, Lotus, Entrust, Netscape, VeriSign, Bull, SPYRUS, Citicorp, SSE, Xcert, CygnaCom Solutions, BBN, CertCo, ValiCert, Cisco, Oracle, and Certicom.

It remains to be seen, however, which companies will actually support the standards once they are adopted. Entrust, Microsoft, Netscape, and other vendors that have been active in the PKIX process have already created products that use public key cryptography for security, so their support for PKIX seems likely. In fact Netscape has announced its intention to support the PKIX standards as the IETF approves them. The key to widespread adoption would be for the rest of these companies to make their products PKIX compliant as well.

How PKIX Relates to Existing Solutions

The difference between PKIX and existing PKI implementations is that PKIX is a comprehensive, open solution that encompasses all aspects of a public key infrastructure. PKIX constrains the broad x509 standard, giving up some flexibility in order to gain interoperability. PKIX includes digital signature standards, certificate and CRL formats, certificate and CRL retrieval protocols, certificate management protocols, directory services, and key management. The advantages of PKIX are its openness and interoperability.

IBM’s High-Level PKIX API

Because PKIX is an open standard, it can use any underlying security protocols. IBM has selected the Common Data Security Architecture (CDSA) for its PKIX implementation, although other protocols, such as Microsoft’s proprietary CryptoAPI, can be used. CDSA was developed by Intel and adopted as a standard by the Open Group. CDSA is an open, modular and flexible standard that easily allows for different levels of security.

IBM is writing a high-level API that provides application programs and administrators a convenient way to invoke the underlying CDSA functions. This API allows developers to write applications that can reliably use public key cryptography for security without being concerned about the details of the PKI implementation.

Why Support PKIX?

IBM plans to support PKIX because it recognizes the need for a PKI standard as a way of boosting public key cryptography technology thereby creating a market for products that support the standard. As evidenced by the recent Congressional hearings on Internet security, there is a pressing need for a comprehensive Internet security solution.

By supporting PKIX IBM is leading the market by making a commitment to promoting interoperability between different products and companies, as well as creating a secure environment for distributed applications.

A Proven, Interoperable, Standard Technology

Public key cryptography has proved its usefulness and robustness as a technology, and the PKIX effort is the best way of obtaining widespread support for it as the basis of Internet security for the next century. Emerging standards for interoperable secure e-mail (S/MIME), Internet commerce, and Java and ActiveX code signing all rely upon public key cryptography.

Interoperability is essential since the platforms that constitute the Internet are so varied. Standards such as PKIX are the best way of assuring interoperability. Adopting a standard approach to security also eliminates the security holes that result from the lack of interoperability of different approaches.

Fuel for Market Growth

IBM believes that in order to create a broad market for the products that use public key cryptography, it is essential to adopt a standard PKI approach. Such an approach will make it much easier for security administrators to manage the potential explosion of keys and certificates that widespread use implies.

Already administrators are complaining about how many certificates they need for various applications. Standardization means a single key management and certificate administration interface, and far fewer certificates. According to the Burton Group Network Strategy Report on Public Key Infrastructure Architecture, “Without solid infrastructure, services like key backup, recovery, and update in enterprise PKI will create management problems that will affect both the scalability and costs of corporate networks.”

Additionally, because a high-level API means that application developers needn’t worry about the implementation details of public key cryptography, they will have a much easier time of incorporating security into their applications, and they will make fewer mistakes, thereby leading to improved security and increased deployment.

What PKIX Means for IBM and its Customers

Adoption of PKIX means that software vendors can speak with a unified voice about their approach to security. It means that IBM and its partners can deliver products that their customers can rely upon to be secure, interoperable, and easy to manage. Rather than deciding among competing technologies and potentially creating security holes in the process, customers can be certain that all products conforming to the PKIX standard will be secure and interoperable. Additionally, customers will receive the benefits of a common management interface for keys and certificates, reducing the associated administrative overhead and increasing their desire for more products that conform to the standard.

Customers have already been introduced to certificate-based security in products such as Lotus Notes, Lotus Domino and Netscape Navigator, and they have relied upon it for SSL-based secure communication. Answering emerging customer needs for secure messaging, commerce, and software distribution are vital to the industry. PKIX is the best way of ensuring that these technologies are developed and deployed in a consistent manner, thereby instilling confidence in customers.

Privacy | Legal | Contact |