

Public Key Infrastructure – Securing the Future of Communication

The electronic world is perhaps the greatest enabler the planet has ever seen. Innovations such as the Internet, e-commerce, e-mail and remote access have made us more efficient and given us unprecedented access to information. With the broad and open arms of the Web come issues of security and trust. Threats of fraud, eavesdropping and data theft have prevented many people from fully embracing the benefits of the electronic world. Public Key Infrastructure (PKI) brings the trust and security of the physical world to electronic transactions and communication.

Origins ... A Brief History of Cryptology

From Rome to Stanford

Julius Caesar used cryptology to secure his post as the eventual leader of Rome

Cryptology is the science of communicating and deciphering secret writings. Julius Caesar used one of the earliest recorded cryptographic systems during Rome's battle at Gaul in 58 BC. Able to securely deliver messages to his commanders, Caesar's campaigns were highly successful and assured his future in Rome.

In 1945, nearly 2000 years later, the National Security Agency and the Central Intelligence Agency began using electronic forms of cryptic communication. It wasn't until 1976 that doctoral student Whitfield Diffie and Stanford professor Martin Hellman developed the concept of a public key cryptosystem. Their paper, entitled "New Directions in Cryptology," would become the foundation of public key infrastructure. In essence, they proposed that two pass-codes or "keys" should be used to decipher messages. A public key would be mathematically derived from a private key. The private key would be virtually impossible to compute from the public key. The public key would be used for securing or "locking" messages and the private key for decoding or "unlocking" them.

MIT to the Federal Signature Bill

Inventors from MIT developed the first usable PKI crptosystem

Soon after Diffie and Hellman's paper was published, three inventors from MIT – Ron Rivest, Adi Shamir and Le Adleman – developed the first usable public key encryption system, complete with digital signatures. Known as RSA, the system became the best known and most widely adopted public key infrastructure cryptosystem.

Public key encryption was first used commercially in the 1980s by financial institutions

By the early 1980s PKI was opening the door for many new business opportunities. Financial institutions adopted public key technology to secure funds transfer networks, and telecommunications and government agencies soon followed. By the mid 1990s, the Internet was showing commercial promise and public key encryption began to flourish.

Today, Web browsers, pagers, personal digital assistants and many other communication devices rely on a public key infrastructure. Recently the United States passed the Federal Digital Signature Bill granting digital signatures the same legal validity as handwritten signatures. The U.S. government also mandated that by the year 2003 all government forms must be able to be posted, signed and filed electronically. These recent developments firmly solidified the future of PKI.

Why the Electronic World Needs PKI

Extending the Security of the Physical World

When sending important documents in the physical world, safeguards such as signatures and sealed envelopes bring a high level of security and trust

In the physical world, when we send an important document – such as mailing a check – there are many safeguards built into the process that help protect us against fraud. For example, imagine you are paying a utility bill. Your signature on the check is a unique and hard to reproduce authorization to your bank to pay the funds to the party in question. The paper the check is printed on also has anti-tamper measures such as watermarks, micro-printing and chemical sensitivity, making it difficult to copy or alter the check. When you mail the check, you might seal it in a security envelope that is difficult to see through. When the receiving party gets the envelope with your check sealed inside, he or she will be able to easily determine if the envelope has been opened or tampered with. If there is any doubt about your ability to pay, the vendor can contact your bank and verify funds. All these processes combined bring a high level of trust and security to a transaction.

When we use the web for purchases (or any other transaction that requires security), many of the security mechanisms we take for granted in the physical world are absent. In many respects, sending an important document electronically is a lot like hitchhiking – your document hops from virtual car to virtual car until it reaches its destination. On the Internet highway, anyone can potentially intercept your message. PKI overcomes these limitations and brings the same security mechanisms from the physical world to the electronic world.

Meeting Legal Requirements

To meet the legal requirements of a contract, electronic documents must be authenticated, secure, private, enforceable and meet non-repudiation conditions

When sending important electronic documents, such as payments or contracts, there are a number of basic legal requirements that bind all parties involved in the transaction and make the documents legally enforceable. The transaction must be:

Authenticated: The sender of the message must be who he or she claims to be and must be authorized to commit his or her organization to the transaction.

Secure: The method of transmitting the message should make tampering easily detectable and preserve the message's integrity.

Private: The document must be protected against improper access or release.

Enforceable: The message must be a permanent document signed by all appropriate parties and must be verifiable.

Non-Repudiation: Both parties must not be able to disavow or deny involvement with the transaction.

A public key infrastructure meets all the legal requirements for the transmission of secure transactions. Applying PKI to the on-line world opens a great window of opportunity.

The Many Applications Enabled by PKI

The possibilities of secure communication with PKI are endless. Examples include:

- E-mail with customers, partners and employees
- Remote access to corporate databases and intranets
- Electronic forms such as purchase orders
- E-commerce including electronic data exchange and financial transactions
- Desktop security to protect files and folders
- Electronic checks
- Digital contracts including leases and mortgages
- Electronic time cards
- Tax forms
- Work-floor automation based on signature linked forms

The Components of PKI

Because any computer data can be converted into binary numbers, the data within any message can be mathematically altered. Thus, electronic messages can be transformed into alternative representations that can create exact replicas of the original. The flexibility of electronic messages bring both positive and negative consequences. The negative possibilities include the ease with which messages can be replicated and transmitted, leading to fraud. PKI enables positive consequences including the ability to easily encrypt, secure, track and decrypt messages, counteracting fraud.

Public and Private Keys

Public and private keys are asymmetric – what one key locks, only the other key can unlock

PKI utilizes a key pair system of asymmetric keys that are mathematically related to each other and perform opposite functions. What one key locks, only the other key can unlock. Public and private keys are unique to each user in a PKI system. The private key is created first. A one-way math function is applied to the private key to generate the public key. It is virtually impossible to determine a person's private key from his or her public key. A real-world, yet simplified example might be a telephone book. If you know the name of the person you are calling, you can easily find his or her phone number. However, if you only know a phone number, it is very difficult to determine the person's name.

Private keys must be protected from compromise and are usually stored on physical devices such as smart cards or tokens. The owner typically carries these physical devices with other real-world keys (such as house, car, etc.).

Public keys on the other hand, are made publicly available. Anyone wishing to send secure messages or transactions would use the recipient's public key as part of the encryption process. Encrypting something with someone else's public key ensures that only that person's private key can decode the message. If a message encrypted with someone else's public key was intercepted, it would be nearly impossible for the message to be unscrambled.

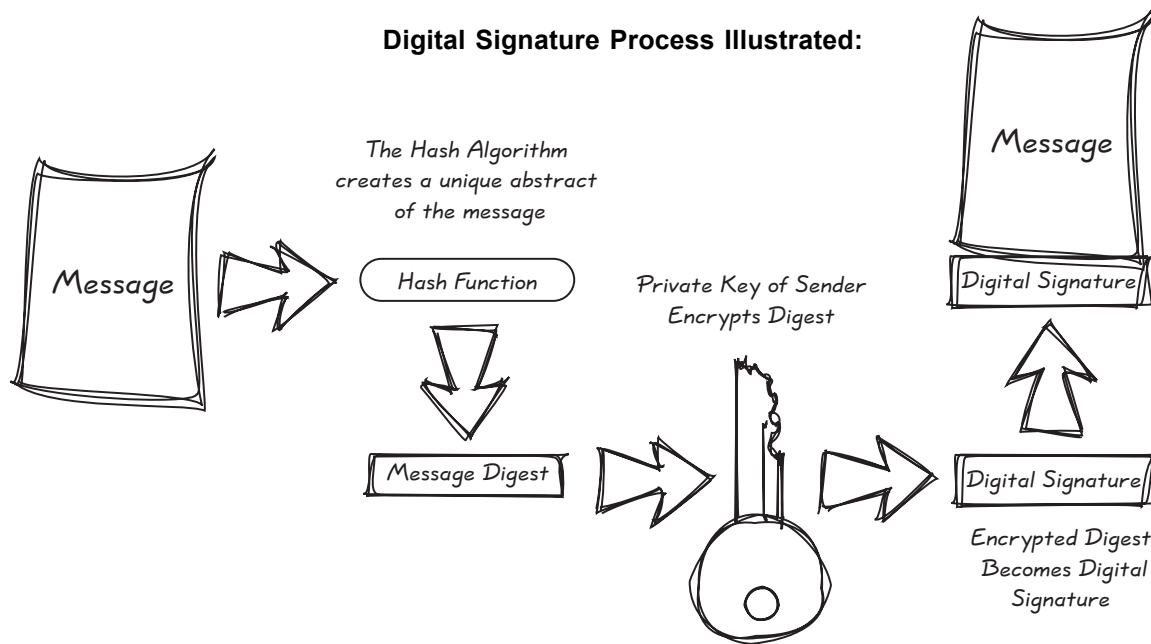
Digital Signatures

Digital signatures identify the sender of the message and verify the integrity of the message

When receiving an encrypted message, it is important to be able to verify that the sender of the message is who he or she claims to be. This is accomplished with a digital signature – a unique message-signing process that reveals the sender's identity and verifies the integrity of the message. Digital signatures are irrefutable, unique to each transaction and are virtually impossible to copy or transfer. Digital signatures are as legally acceptable as a hand-written signature on a contract.

The signature is a mathematical function that involves the original message and the sender's private key. The first step in the signature process involves performing a math algorithm known as a *hash function*. The hash function takes the original message and reduces it to a fixed-length, 160-bit string of characters known as a *message digest*. The message digest is essentially a mathematical abstract of the original message. If a single character in the original message changes, the message digest changes significantly. The message digest is then encrypted with the sender's private key. The resulting encryption is known as the digital signature. This signature is unique to each message and is appended to the original message.

Digital Signature Process Illustrated:



The Encryption Process

Commercially encrypted messages are scrambled using keys that are difficult to decode

The next stage of the PKI process is securing the message and its signature. This is accomplished by scrambling or *encrypting* the message and signature. Encryption involves a unique mathematical process that transforms data into a scrambled message that requires an encryption key to unlock it. The strength of the key depends on its number of bits. For example, a 20-bit encryption key has 1,048,576 possible variations. Although this seems like a hard key to crack, a normal computer can process a million key combinations very quickly and guess the code. The advancement of computers has led to the need for higher bit encryption. In the year 2000, the commercial standard for strong encryption is 128-bit which has 680,565,000,000,000,000,000,000,000,000,000 possible variations. Experts estimate that 2048-bit encryption will soon be the commercial standard as existing super computers can break 1024-bit encryption in 20 years.

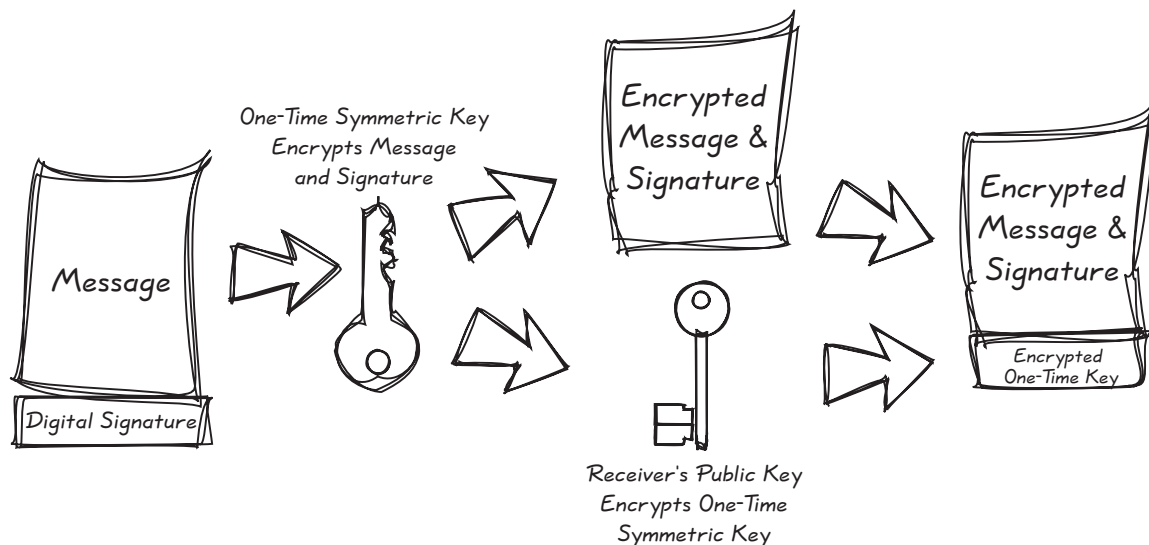
Transporting Encryption Keys

Securely transporting encryption keys is critical to maintain the privacy of encoded messages

Once the message and signature is encrypted, the next process is to securely transport the key required for decrypting the message. The key type used in message encryption is known as a *symmetric key*. A symmetric key is a unique key created for a one-time use that is able to both lock and unlock a message. Both the sender and the receiver will need the same symmetric key to encode and decode the message. When transporting a symmetric key, it is critical to keep the key out of the hands of everyone except the intended recipient. If the symmetric key were to fall into the wrong hands, the message could easily be decrypted, compromising the privacy of the message.

PKI adds an extra layer of security by encrypting the one-time symmetric key with the receiver's public key so only the receiver can decode the symmetric key with his or her private key. The encrypted one-time symmetric key is appended to the encrypted message and the message is now ready to be sent.

The Encryption Process Illustrated:



Digital Certificates

Digital certificates are electronic forms of ID that certify the holder's identity

Digital certificates, or public key certificates, serve as the equivalent of a birth certificate or a passport for electronic identity. Digital certificates are electronic forms of identification that can be validated by a recognized authority. All users of PKI must have this form of registered identification. Certificates can contain a variety of information, including the certificate holder's name, public key, expiration date of the certificate, operations the public key can perform (encrypt, decrypt or verify digital signatures), the issuer's digital

signature, serial number and encryption method. Digital certificates are used to authenticate or verify that the user is who he or she claims to be. Certificates are publicly posted on-line by third parties known as *certificate authorities*.

Certificate Authorities

Certificate authorities are trusted third parties that vouch for the identities of digital certificate holders

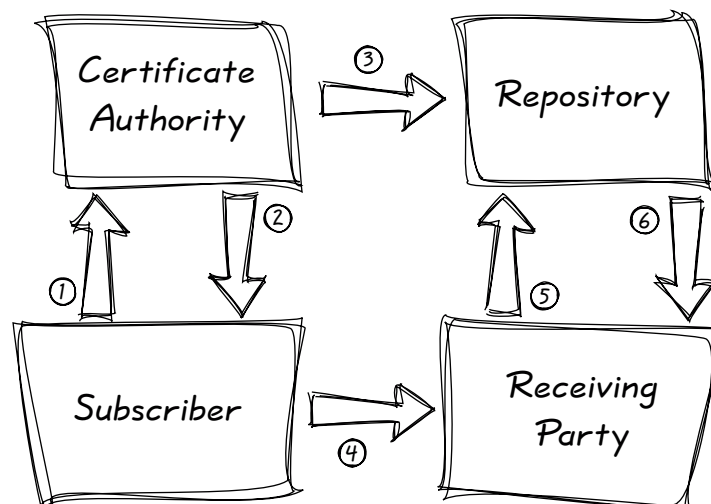
A certificate authority (CA), a trusted third party, is the electronic equivalent of a passport office. The primary purpose of a CA is to issue digital certificates and to confirm the identity of the person associated with a certificate. CAs bring an added level of trust to PKI-based transactions.

The role of the CA can be better understood by using an analogy to a real world passport office. A passport office issues a passport, a secure document that certifies the person holding the passport is who he or she claims to be. Any country that trusts the authority of the passport holder's passport office will also trust that individual's passport. The passport office is a third party that vouches for the identity of the person in question. The function of a CA is the same as that of a passport office – a trusted third-party authority.

The Certification Process

The certification process is as follows (see supporting illustration on next page):

1. Subscriber (sender) applies to CA for digital certificate.
2. CA verifies subscriber's identity and issues digital certificate.
3. CA publishes certificate to public, on-line repository.
4. Subscriber signs message with private key and sends message to second party.
5. Receiving party verifies digital signature with sender's public key and requests verification of sender's digital certificate from CA's public repository.
6. Repository reports status of subscriber's certificate.



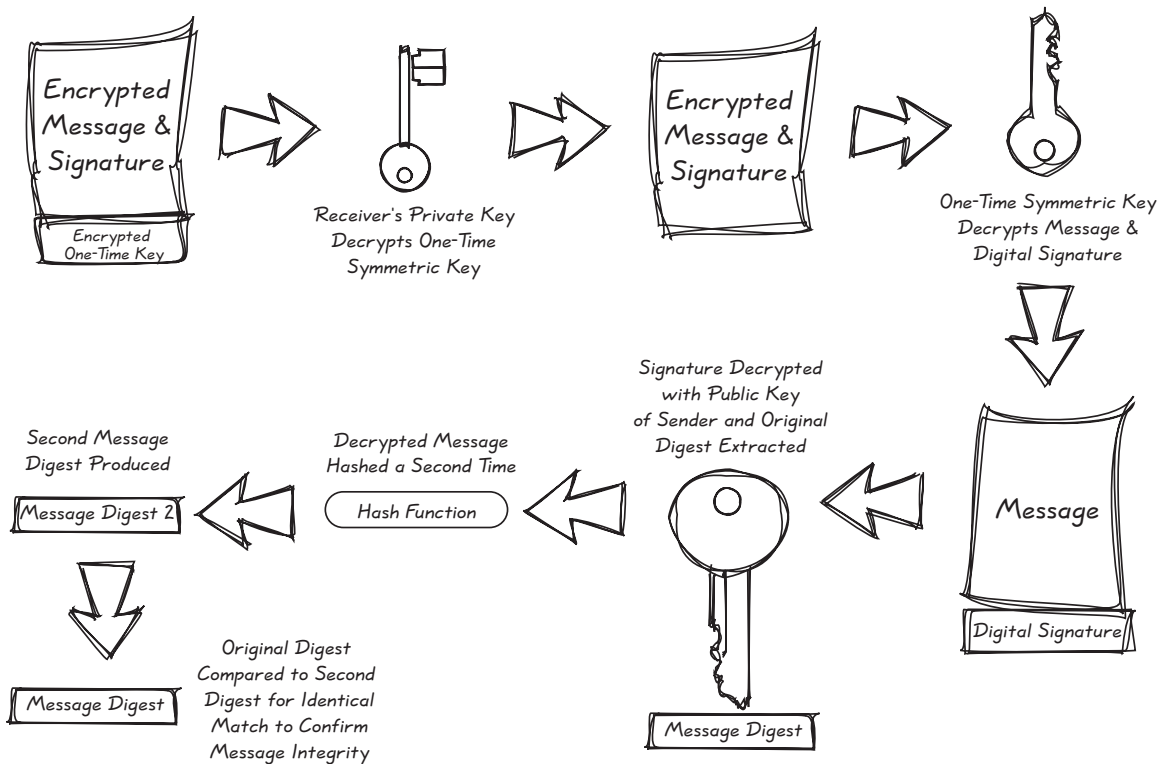
Message Decryption and Verification

After a message has been received, it must be decrypted and its contents must be verified as unchanged

After the signed and encrypted message is received, the message is decrypted and its content integrity is verified. The one-time symmetric key that was used to encode the message is unscrambled using the receiver's private key. The symmetric key is then used to decode the encrypted message and signature.

Using the public key of the sender, the digital signature is decrypted and the digest for the message is extracted. The message digest serves as a file integrity checksum later in the process. The decrypted message is checked to see if its contents are exactly as they should be through a repeat of the hash function. The result of the hash algorithm is a second message digest. If that second digest perfectly matches the original digest, the message integrity is confirmed and the message has been successfully transmitted.

Message Decryption and Verification Process Illustrated:



An Application of PKI – On-line Banking

The Problem

Most on-line banks rely on user name and password authentication methods that are easy to impersonate and difficult to track

In the United States, on-line banking has become popular, yet consumers are still very concerned about their privacy and security. Most on-line banking sites rely on a user name and password to authenticate customers. Early implementations experienced serious problems with unauthorized users transferring money from unsuspecting customer accounts.

The user name and password method of authentication used by most on-line banks is also known as *single factor* authentication. The security problems with single factor authentication are many. For example, passwords are often easy to guess or find, making user impersonation common and easy to accomplish from anywhere in the world. In addition, many consumers use the same password across multiple web sites and applications. If a password is compromised at one point, it could potentially be used at many other points. For example, if an e-mail password was discovered, it might not be difficult to use that same password at the user's bank. With some financial institutions, the liability regarding on-line banking fraud rests with the user rather than the bank. In these cases, the customer ends up at a loss and has little recourse. Single factor authentication also has no tracking mechanism, making it virtually impossible to determine who impersonated the customer.

The Solution

With PKI based on-line banking, physical tokens are used to authorize and digitally sign every transaction

With a two-factor secure PKI solution, on-line banking will become a highly secure and trusted way of handling monetary transactions. With PKI, a physical device, such as a token, must be plugged into a port, such as a USB port, and activated with a unique pin number. That PKI device contains the users digital certificate, which replaces the user name. The pin number associated with the PKI token device replaces the password.

With PKI, every transaction is digitally signed and stored by the bank. Now, a user identity can be verified and tracked. Because tokens are physical devices, similar to ATM cards, as long as the user has the token, they can rest assured that only they have the ability to authorize the transaction. If the pin number is compromised, a new token and pin number can be issued, just like a bank might do if an ATM card pin number is compromised.

The end result of a PKI banking solution is significantly reduced fraud, server verified user logins and long-term tracking via stored transactions. Authentication, authorization and non-repudiation are benefits unique to PKI that will enable the future of on-line banking.

Summary

Benefits of PKI

PKI brings the security and trust of the physical world to the electronic world. Through strong encryption, asymmetric keys, digital signatures and trusted third-party verification, PKI meets the legal standards required to conduct verifiable and secure on-line transactions. Benefits include:

- Confidential communication: Only intended recipients can read files.
- Data integrity: Guarantees files are unaltered during transmission.
- Authentication: Ensures that parties involved are who they claim to be.
- Non-repudiation: Prevents individuals from denying involvement in a transaction.

PKI creates a climate where information piracy and fraud are absent and both parties accept legal standards. PKI is a catalyst that will lead to greater acceptance of Internet-based products and services.

The Rainbow Advantage

Founded in 1984, Rainbow Technologies is a leading provider of security solutions for the Internet and e-commerce. Rainbow products bring high-performance, secure, PKI-based solutions to end-users and corporations.

Rainbow's CryptoSwift Hardware Security Module (HSM) is a tamper-resistant hardware solution that provides secure key generation, secure key storage and authentication. CryptoSwift HSM uses Rainbow's FastMAP chip, the world's fastest public key cryptography integrated circuit, to provide high-performance, cost-effective cryptography for applications such as virtual private networks and financial processing.

Rainbow's iKey2000 product is a USB-based portable PKI authentication token that generates and stores a private key and digital certificate on a device small enough to fit on a key chain. More advanced than a smart card, the iKey2000 simply plugs into any USB port and provides strong user authentication without the need for costly reader devices. The iKey2000 was designed to support a wide range of desktop applications and portable systems.

For more information about Rainbow Technologies and Rainbow products, visit www.rainbow.com.