Schlumberger

Technology Brief: Public Key Infrastructure (PKI)-A Primer

by David Storch

PKI Principles

- ➤ Symmetrical key systems use a shared secret key to encrypt and decrypt messages. A separate secret key is needed for each correspondent pair
- ➤ Asymmetrical key systems use a public/private key pair to encrypt and decrypt messages
- ➤ Even though a mathematical relationship exists between the public and the private key, it is practically impossible to derive the private key from the public key
- ➤ Only the owner has access to the private key, while the public key is openly available to everyone
- ➤ The private key can also be used to create a digital signature that is used to authenticate the sender of a message
- ➤ If information is encrypted using the public key of its intended recipient, only that person can decipher it

As the Internet becomes an increasingly important means of conducting transactions and the volume of e-business grows exponentially, a secure infrastructure is needed to provide authentication, confidentiality and access control. Security has evolved from a basic password scheme to a complex key infrastructure. Initially, shared secret keys were exchanged and maintained between pairs of correspondents. However, as the Internet expanded, this method became impractical. Today, a powerful public-private key technology (PKI or Public Key Infrastructure) has evolved to solve this problem.

The Challenge

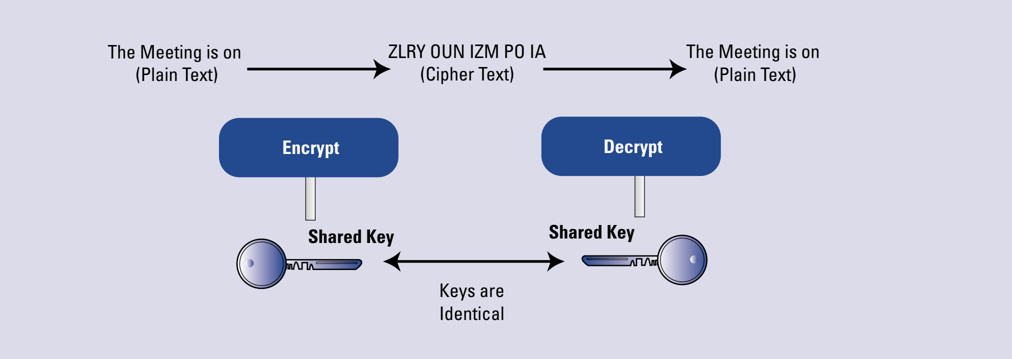
Years ago, facility security could be achieved by placing guards at the front doors, performing background checks on employees and locking file cabinets. Today, facilities are scattered around the globe, yet dispersed personnel in these facilities need to communicate in real time. Additionally, virtual offices exist on customer premises and in employees' homes or hotel rooms. Thus, confidential data needs to be shared via the Internet, and critical information is transmitted through ordinary telephone lines. The ability to communicate, share data and execute transactions instantly with anyone, anywhere in the world is not without a price. There is a potential for fraudulent access to sensitive data or transactions.

How do users know that the people they are communicating with are actually who they claim to be? Can a third party "eavesdrop" on the electronic interchange and capture a credit card number or key business intelligence? Consumers must wonder if the site they are sending their confidential data to is the legitimate web site of a reputable firm. Businesses must ensure that transactions processed on their sites are not fraudulent and that their corporate Intranets are available only to trusted parties. These are fundamental questions in network security. All of these issues involve authentication, or ascertaining the true identity of the person on the other end of an electronic interchange.

Symmetric Keys

Before PKI, confidentiality and authentication were typically addressed via encryption systems using symmetric keys (see Figure 1). To encrypt and decrypt electronic messages and files, senders and receivers alike used symmetric, or identical, keys. For access control, hosts typically

Figure 1: Symmetric encryption (using a shared key)



DeXa
Suite of Services
Enabling the promise of the digital enterprise

stored user passwords in a database, either encrypted or in cleartext, in order to match them to user login attempts. Although these systems are easy to understand and implement, they are no longer adequate.

Password Inadequacies

Passwords are easily deduced, or "cracked." Readily available shareware can derive passwords with success rates of over 70%. To make passwords easy to remember, people typically use common words or names, which can then be cracked by dictionary-based attacks or by other cryptoanalysis schemes. A company may require complex passwords (mixed case, digits, punctuation marks) to overcome the cracking problem, but more complex passwords are easily forgotten, resulting in employee downtime and increased IT-support costs to reset or reissue passwords. If employees have dozens of passwords, as they often do, the problems and costs associated with forgetting them are further exacerbated.

Symmetric key systems do not scale well either. A "secure" channel, such as a phone line or a secured envelope, is required to distribute the secret key, which means that for environments as large as the Internet, millions of secure channels must be established. The result is a complex, inefficient many-to-many mesh of clients and servers sharing symmetric keys. Identical copies of keys must exist somewhere outside of the end-user, making those keys vulnerable.

How PKI Works

PKI has evolved to address the issue of large-scale distributed authentication. Unlike symmetric key systems, PKI can scale well while avoiding the costs and inconveniences of password loss.

In a PKI system, instead of having a single key that needs to be shared, a user employs a tool that generates a pair of mathematically related keys: the public key and the private key.

The public key is openly and readily available to anyone who wants it–precisely the opposite of the classic system in which the key must be closely guarded. Therefore, it can be stored on any computer, directory or database. The public key of the receiving person or system is used to encrypt transactions, documents and passwords.

The private key, by contrast, belongs solely to its owner, who stores it on a secure device, such as a tamper-proof smart card. No other person or entity ever possesses the private key, nor needs it — not even the server authenticating the end-user. (In some PKI systems, however, the private key may be backed up in encrypted form in order to facilitate recovery, should it be lost.)

A message encrypted with the recipient's public key–which is listed in a directory–can only be decrypted with the recipient's private key. This ensures confidentiality. Conversely, the private key of the sender can be used to electronically sign documents. If the signature can be decrypted using the sender's public key, the receiver is assured that the message is legitimate–the sender alone possesses the private key to encrypt the signature. Thus, access to the private key replaces the use of a password, and the public and private keys can be used together to secure transactions that need to be both confidential and authenticated.

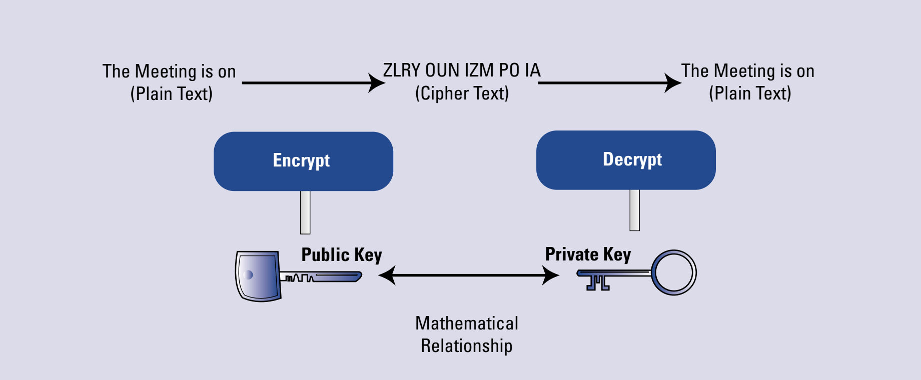
The private key is not shared in a PKI system. Despite today's high-speed computational technologies, deriving the private key from knowledge of the public key is practically impossible–the mathematical relationship between the two keys is too complex. While the Internet is not a secure infrastructure, PKI makes it "virtually secure."

Benefits

The ramifications and benefits of PKI are many, and new ones are still being discovered and leveraged. For example, digital signatures encrypted with private keys are becoming as binding as handwritten signatures. Real-time, online authorization is now possible, enabling users to sign electronic items such as checks, expense reports and legal documents without incurring the delays and costs of transmitting signed documents. In one of its white papers, Entrust estimates that companies can save an average of $3 million in paper processing costs by moving away from paper and towards electronic forms. Yet legal requirements and business needs mean that unsecured e-forms are unacceptable.

Lastly, an estimated 10% of all online transactions are fraudulent, and during the week of Christmas 1999, approximately $100 million worth of bogus transactions were made. Even a partial reduction of such fraudulent transactions can save companies many millions of dollars, and PKI is well-positioned to provide the security framework for the new economy.

Figure 2: Asymmetric encryption (using a public and private key)



Other product and company names mentioned herein may be trademarks of their respective owners.