Whitepaper

Public Key Infrastructure (PKI): A High-level Overview

Secure data is constantly being sent over public networks like the Internet. How, then, can users be sure their sensitive data will be protected and will only be accessed by the intended party? Any compromise or theft of sensitive data could mean millions of dollars in damages, or even the downfall of a company. In order to protect this information, users can encrypt their data, making it unreadable to anyone but the intended party. A public key infrastructure, or PKI, allows users to privately exchange sensitive data over public spaces by encrypting the data with a public and private cryptographic key pair that is created and shared through a trusted device, allowing both parties to be confident their sensitive data is protected.

What Is PKI?

A Public Key Infrastructure, which works by using asymmetric encryption, allows users to securely transmit sensitive data over insecure public spaces such as the Internet. By using PKI, this data is both encrypted and authenticated, enabling the recipient to be assured of the confidentiality and integrity of the message.

Public key infrastructures use public and private key pairs that are generated and distributed by a trusted device known as a certificate authority. Certificate authorities, which are often validated by third-party auditors, are used to generate digital certificates and assign them to the electronic devices that make up the PKI.

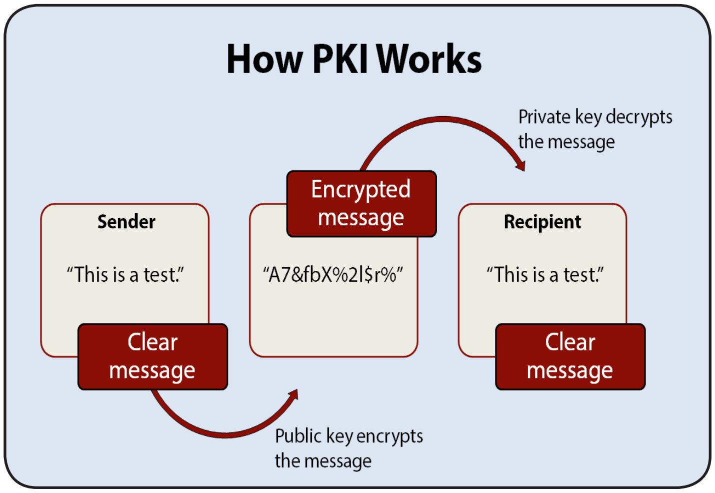
A certificate is made up of two parts: a public key and a private key. The public key is used to encrypt data and the private key is used to decrypt it. Public keys can be widely distributed without fear of compromise because public keys cannot decrypt data. Only the private key, which must be carefully protected, can successfully decrypt the message. When a single party provides their public key to another, it enables a "one-way" channel to transmit data. When both parties exchange public keys, they are able to send trusted communication back and forth.

When all parties in a PKI are authenticated using the same certificate authority, a circle of trust is established. The entire certificate management lifecycle can be performed by the same certificate authority: introducing new trusted parties, revoking certificates from unauthorized parties, storing certificates, and periodically issuing new credentials upon their expiration.

How Does PKI Work?

Parties wishing to confidentially send data to one another begin by exchanging public keys. Using the receiver's public key, the sender encrypts their message and sends it to the receiver. Only the receiver's private key can decrypt the message. The two keys are related mathematically, but the private key cannot be derived from the public key, so there is no chance of compromise by sharing it. The private key, however, should never be shared under any circumstance.

These certificates are also used for signing and verifying secure data to ensure message integrity. In these cases, the private key is used to sign the message, which generates a certificate that contains information about the key, including the key owner's name. This certificate is sent along with the signed data to the receiver. The public key, which is available to all users, is used to verify the received data, ensuring that it came from a trusted source and was not forged.


How PKI Works