**Public Key Infrastructure (PKI)**

A security architecture called Public Key Infrastructure (PKI) was designed to offer a higher degree of security for information exchange over the Internet.

It is defined in 2 ways:

The process, tools, and technology involved in building a secure data infrastructure.

The verification of content and authentication using a pair of public and private keys.

**Benefits of PKI**

Assurance on the quality of data transmitted through electronic means.

Assurance on the information's source and final destination.

Assurance of the time and timing of such information.

Certainty of the privacy of such information.

Assurance that such information may be used as evidence in a court of law.

**Use of PKI**

To support secure information exchange over insecure networks.

e.g., the Internet where such features cannot be provided easily.

For information exchange over private networks.

e.g., an organization’s internal network.

To securely deliver cryptographic keys.

To facilitate other cryptographically delivered security services.

**How Does PKI work?**

PKI uses a mathematical technique called public key cryptography.

Pair of related cryptographic keys are used.

Verifies the identity of the sender (through signing).

Ensures privacy (through encryption of data).

**Services provided by PKI**

Ensures privacy between sender and receiver of the data by directly preventing unintended disclosure of the data.

Identifies the sender of the data by authentication.

Ensures that the data has not been modified or altered with.

**Public Key Cryptography**

Uses a pair of mathematically related cryptographic keys.

One key is used to encrypt information.

Only the related key can decrypt that information.

Knowledge of one key does not allow you to calculate the other.

**Public keys and private keys**

The public key is made public, it is freely distributed and can be seen by all users.

The private key is kept secret and is not shared amongst users.

Your private key enables you to prove that you are who you claim to be.

**Encryption methods**

**Asymmetric**

Two keys, one each for encrypting and decrypting.

Able to identify the sender and recipient using encryption and decryption using a private key known only to one of the entities involved in the communication.

**Symmetric**

Same key for encrypting and decrypting.

Since everyone involved knows the same key, it cannot be used to identify the sender or the recipient.

**Digital Signature**

A digital signature is a unique, encrypted numerical value.

It differs each time it is generated and is used to prove the ownership or copyright of data.

**Using a private key for signature**

A hashing algorithm is performed on the document to be signed producing a unique numerical value.

After that, it is encrypted with a private cryptography key, and the outcome is connected to the document.

The encrypted value is sent either at the end of the data or as a separate file with the message.

The corresponding public key may also be sent either on its own or as a certificate.

Does not provide anonymity because data that is digitally signed or encrypted can be simply read, processed, and the signature checked by anybody who receives it.

**Using a public key for Signature**

The hash value that was calculated by the sender for the data is decrypted by the recipient using the correct public key.

The hash value of the received data is then computed using the hashing algorithm.

When the freshly calculated hash value and the hash value calculated by the sender match, the recipient is informed that the data was sent by the private key owner at first and hasn't been altered after it was signed.

**Digital Certificate**

A digital document that binds your public key to an identity that the issuing Certification Authority (CA) is willing to vouch for.

**Digital Certificate Usage**

A digital certificate issued by one of the public CAs will contain information in the key usage field of the certificate.

This means that the private key may be used for specific purposes such as:

* digital signatures
* certificate signing
* encipher or decipher only
* key encipherment
* data encipherment

**Certificate Standards**

The data in a certificate usually conforms to the ITU (IETF) standard X.509.

Includes information about:

* the identity of the owner of the corresponding private key
* the length of the key
* the algorithm used by the key
* the associated hashing algorithm
* dates of validity of the certificate
* the actions that the key can be used for

**The Component of PKI**

Certification Authority

* Issues and verifies digital certificates

Revocation

* There is a system for making it known that certificates are no longer valid (revoked).

Registration Authority

* A third-party used by a Certificate Authority to perform checks on the person or company applying for the certificate

Certificate Publishing Methods

* PKI systems require the publishing of certificates so that users can find them.

Certificate Management System

* Systems that manage certificates:

PKI-aware Application

* Applications are those that have had a particular CA software supplier's toolkit added to them.

**Certification Authority (CA)**

issues and verifies certificates.

Takes responsibility for verifying that the individual requesting a certificate is who they say they are.

verifies the accuracy of the certificate's information and digitally signs it.

**Generating Key Pairs**

For their client, the CA may generate a public key and a private key.

As an alternative, the certificate applicant may create their own key pair and send a signed request to the CA along with their public key.

**Issuing Digital Certificates**

The CA will make a variety of checks to prove your identity.

The quality of the checks performed before to the certificate's issuance may be disclosed by the CA.

The CA may be:

* Part of the organization requiring a digital certificate (issuing their own certificate)
* A company (e.g., a bank or a post office)
* An independent entity that is widely trusted for that purpose (e.g.VeriSign)

Different levels of these checks correspond to different classes of certificates that can be purchased.

**Digital Certificate Classes**

Class 1: Providing an email address makes it simple to obtain certifications.

Class 2: certificates require additional personal information to be supplied.

Class 3: Certificates are only available for purchase following thorough inspections.

Governments and organizations requiring very high levels of verification can use a 4th class.

**Verifying Digital Certificates**

The CA signs the public key certificate to protect it against modification or fraud.

This is used when checking the public key is valid.

The 'Root CAs' list seen in different 'PKI aware' programs, including your browser, is used to validate the signature.

The public certificate included in the rcot CA list is immediately used for certificate validation.

**Revocation**

There is a system for making it known that certificates are no longer valid (revoked).

A system of revocation lists has been developed that exists outside the directory/database that stores certificates.

Revocation lists may be publicly available as certificates may have been widely distributed.

**Registration Authority (RA)**

A third-party used by a e certificate Authority to perform checks on the person or company applying for the certificate.

Their role is to ensure that they applicant is who they claim to be.

RAs may appear to the requestor of the certificate as CAs but they don't digitally sign the certificate.

**Certificate Publishing Methods**

There are two means of doing this:

* Publishing it in the equivalent of an electronic telephone directory
* Sending it to parties who might need it

**Publishing in Directories**

Directories are databases that are X.500/LDAP compliant.

* The databases contain certificates in the X.509 format.
* They provide specific search facilities which are specified in the LDAP standards published by the IETF.

Directories can be public or remain private:

* Private directories usually contain confidential data that the owner does not wish to be publicly accessible.
* Public directories contain information which can be read by anyone with access to them.

**Publishing Databases**

Databases can be configured to accept X.509 format certificates.

This can be done for private systems where search methods do not follow the LDAP structure.

This method is not used for public directories because it is essentially a proprietary system.

**Sending to Potential Users**

Certificates can be sent through email so that the recipient can add them to their server or desktop.

Certificates can also be carried in portable storage media such as:

* DVDs
* CDs
* USB storage devices

**Certificate Management System**

Systems that manage certificates:

* publish
* suspend
* renew
* Revoke

Do not usually delete certificates because they may be required for future legal reasons.

Typically, a CA will run these systems to keep track of their certificates.

**PKI Aware Applications**

Applications are those that have had a particular CA software supplier's toolkit added to them.

* Enables them to use the supplier's CA and certificates to implement PKI functions.

These applications have no knowledge base built in to them about what the security requirements really are, or which PKI services are relevant in their delivery.