PKI (public key infrastructure)

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party.

Sensitive information can still be encrypted and sent without PKI but there would be multiple security issue such as:

1) Privacy (Interception)

2) Authentication (spoofing)

3) Integrity

4) Non-repudation

Examples of security algorithm:

Symmetric Algorithms: Triple-DES, DES, RC2

Public Key Algorithms:

RSA, DSA, Diffie-Hellman, Elliptic Curve

Hashing Algorithms: SHA-1, MD5, RIPEMD

Elements of PKI:

A typical PKI consists of hardware, software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates. Digital certificates are at the heart of PKI as they affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate.

Elements of PKI:- A typical PKI includes the following key elements:

1) A trusted party, called a certificate authority (CA), acts as the root of trust and provides services that authenticate the identity of individuals, computers and other entities
2) A registration authority, often called a subordinate CA, certified by a root CA to issue certificates for specific uses permitted by the root
3) A certificate database, which stores certificate requests and issues and revokes certificates
4) A certificate store, which resides on a local computer as a place to store issued certificates and private keys

Issues with PKI:

PKI helps in verifying the identities on a network. However, there are various standards that cover aspects of PKI e.g. the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework but there is no singular governing body enforcing the standards. If one CA is compromised, the security of the entire PKI is at risk.

E.g. Web browser vendors were forced to blacklist all certificates issued by the Dutch CA DigiNotar after more than 500 fake certificates were discovered.

What is a Digital Signature?

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

The Hash uniquely represents the original data.

The probability of producing the same Hash with two sets of different data is <.001%.

Signature Process is opposite to Encryption Process

Private Key is used to Sign (encrypt) Data

Public Key is used to verify (decrypt) Signature

Digital Signature Process

Step 1. Hash (digest) the data using one of the supported Hashing algorithms, e.g., MD2, MD5, or SHA-1.

Step 2. Encrypt the hashed data using the sender's private key.

Step 3. Append the signature (and a copy of the sender's public key) to the end of the data that was signed.

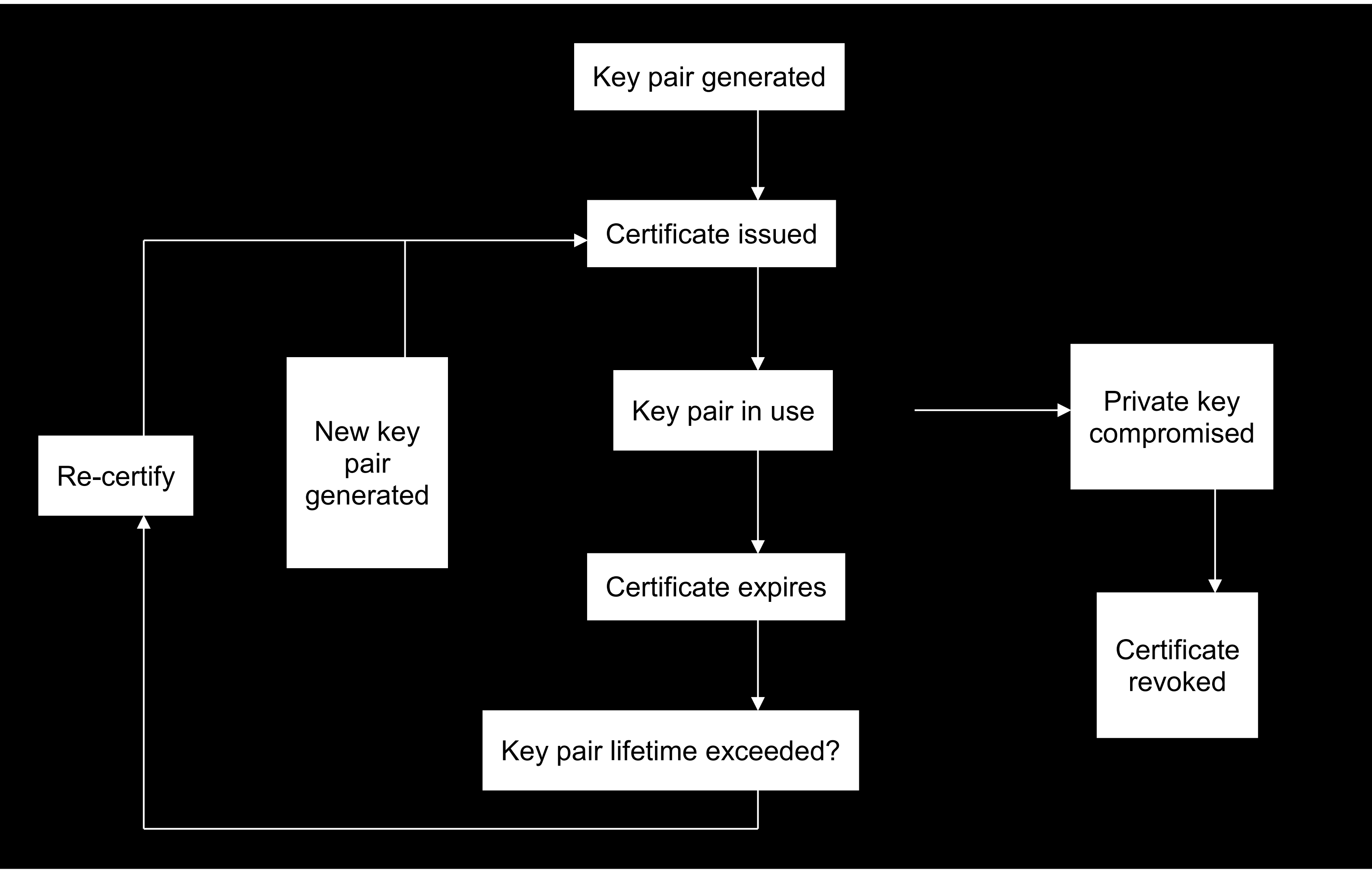
Digital Certificates

Before B accepts a message with A's Digital Signature, B wants to be sure that the public key belongs to A and not to someone masquerading as A on an open network

One way to be sure, is to use a trusted third party to authenticate that the public key belongs to A. Such a party is known as a Certification Authority (CA)

Once A has provided proof of identity, the Certification Authority creates a message containing A's name and public key. This message is known as a Digital Certificate.

Certificate Life Cycle


Key pair generated
Certificate issued
Key pair in use
Private key compromised
New key pair generated
Re-certify
Certificate expires
Certificate revoked
Key pair lifetime exceeded?