Public Key Infrastructure

Josh Wilcox (jw14g24)

March 21, 2025

Table of Contents

Digital Certificates

- A digital certificate **binds** a user or a company to its public key
- Allows for certainty in the identity of senders and receivers
  - Makes the sender know for sure they have the right public key for the recipient to **send and encrypted method**
  - Makes the recipient know the senders key to validate a digital signatures
- Consists of a public key and a user ID of the owner
- Includes a **signature** of an **issuer** (a trusted third party)
  - If the device examining the certificate trusts the issuer and finds the signature to be a valid signature of that issuer, then it can use the included public key to communicate securely with the certificate's subject

Digital Signature Applications

- Secure Email
  - S/MIME (Secure/Multipurpose Internet Mail Extensions)
  - PGP (Pretty Good Privacy)
  - Ensures message integrity and authentication
- VPNs
  - IPsec authentication
  - Certificate-based client authentication
  - Prevents man-in-the-middle attacks
- Wi-Fi
  - WPA2/WPA3 Enterprise authentication
  - EAP-TLS protocol uses certificates
  - Secures wireless networks against unauthorized access
- Web Servers
  - SSL (Secure Sockets Layer)
    - Legacy protocol for HTTPS connections
    - Replaced by TLS for security reasons
  - TLS (Transport Layer Security)
    - Enables encrypted HTTPS connections
    - Server authentication using certificates
    - Client certificates for mutual authentication
- Network Auth
  - 802.1X authentication
  - RADIUS server certificate validation
  - Smart card authentication systems
- Code Signing
  - Validates software authenticity and integrity
  - Used in mobile app distribution
  - Prevents malware distribution through tampered software

Public Key Infrastrucutre

- Set of hardware, software, people, processes, policies and procedures
- Manages digital certificates based on assymetric cryptography
- Enables efficient acquisition of public keys

Certification Authorities

2. Public Key Infrastrucutre
   - Certification Authorities
   - Rgistration Authority
   - PKI Repositories

- Issues, revokes, and distributes certificates
- Often a trusted third-party organisations
  - Verisign
  - DigiCert
  - Comodo
- Certificates are **Signed with the CA's Private Key**
  - Everybody can check the authenticity of the certificates by using the CA's public key
  - This verificat ion works because:
    - The verification process involves using the public key to decrypt the signature. If the decrypted signature matches the hash of the certificate, it confirms that the certificate was indeed signed by the CA
    - **Private Key Signs, Public Key Verifies**
    - If someone "encrypts" (more accurately, signs) a message with their private key, it can be decrypted (verified) using their public key.
    - This does not ensure confidentiality but instead proves that the sender indeed signed the message and that it hasn't been altered.

Rgistration Authority

- Acts as a mediator between users and the Certification Authority (CA)
- Verifies the identity of entities requesting certificates
  - Ensures that the entity is legitimate and authorized
  - Collects and validates necessary documentation
- Does not issue certificates directly
  - Forwards verified requests to the CA for certificate issuance
- Plays a critical role in maintaining trust within the PKI
  - Ensures that only authenticated entities receive certificates

PKI Repositories

2. Public Key Infrastrucutre
   - Certification Authorities
   - Rgistration Authority
   - PKI Repositories

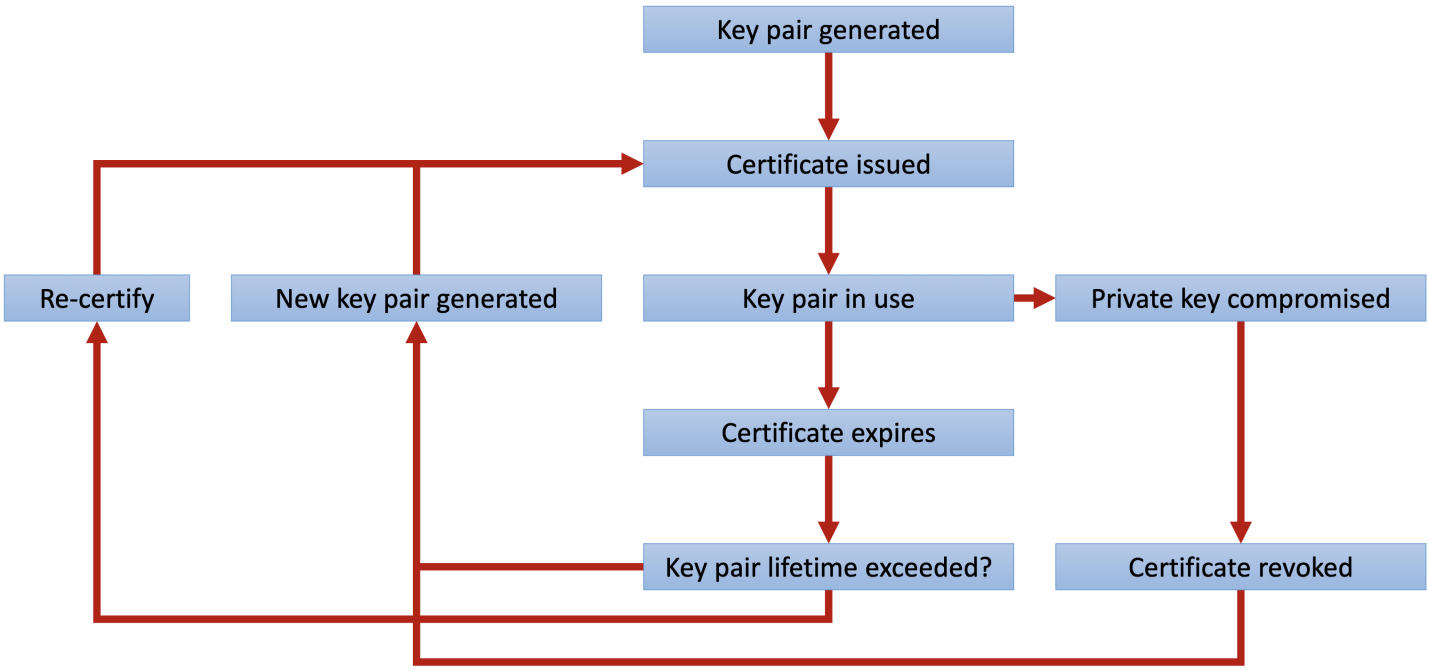
- Stores and distributes certificates and certificate revocation lists
- Manages updates to certificates
- Allows relying parties to retrieve certificates and revocation lsits

Certificate Usage

Certificate Issuance and Usage

- Issuance
  - RA verifies subject information
  - Public-Private key pair is generated
  - CA issues the certificate
- Usage
  - Service fetches the certificate
  - Fetches the certificate revocation list
  - Checks certificate against CRL
    - Checks whether the certificate is still valid
  - Checks the signature of the issuer using the certificate

Certificate Life Cycle

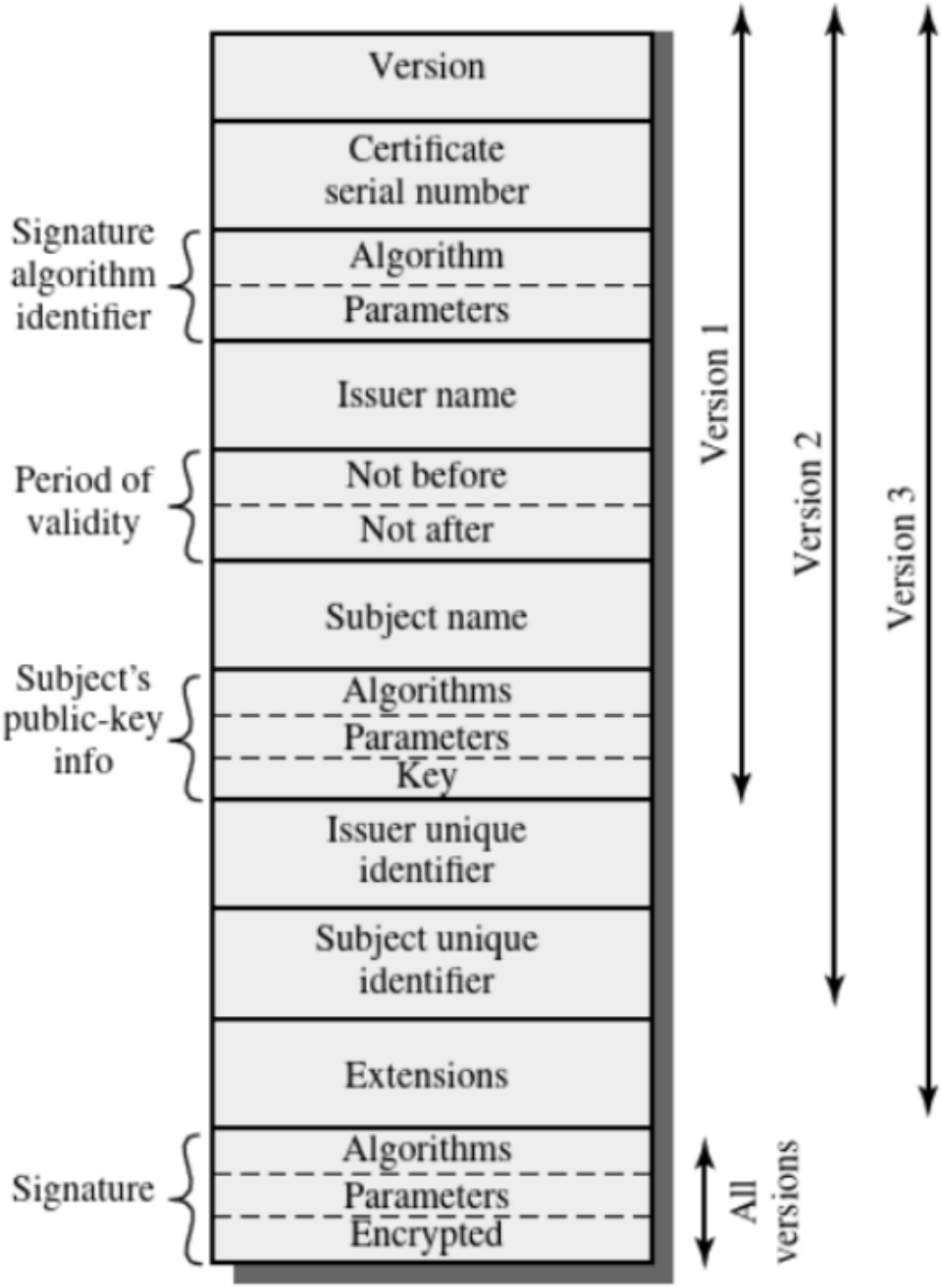


Certificate Revocation

- Certificates may need to be revoked for many reasons
  - CA **Private Key** compromised
  - Human Resources Reason
    - Employees leaving
  - Company ID information changes
- **Certificate Revocation List** (CRL)
  - List of invalid certificates
  - Published regularly by the CA in the PKI repository
  - Sent to any relying party
  - Is not without its problems
    - Not issued frequently enough to prevent an attacker to abuse certificates that need revoking
    - Expensive to distribute
    - Vulnerable to DoS attacks

X.509

- Most widely accepted **format** for public-key certificates
  - Used in IP security, SSL, and TLS
- Issued by the CA
- The signature is the hash of the entire block signed by the CA's private key



X.509 Revocation

- Each entry in the list contains a serial number of the certificate
- Also contains the date
- Very few applications use this due to overheads in storing the lists
- Instead most use the Online Certificate Status Protocol
  - **Direct Query** to the CA asking whether a specific certificate is valid

PKI Attacks

Comodo Case

- In March 2011, attackers compromised a Comodo reseller account
- Fraudulent certificates were issued for high-profile domains
  - Examples include Google, Yahoo, Skype, and Microsoft
- Attackers were able to impersonate these services
  - Could intercept sensitive user data
  - Perform man-in-the-middle (MITM) attacks
  - Craft fake web pages that appeared legitimate
    - These pages would use the fraudulent certificates to display valid HTTPS indicators (e.g., padlock icon)
    - Users would trust the fake pages, believing they were interacting with the legitimate services
    - This could lead to the collection of login credentials, personal information, and other sensitive data
- Possible consequences:
  - Widespread loss of trust in PKI systems
  - Compromise of user credentials and sensitive information
  - Potential for large-scale phishing attacks
- Why these consequences were possible:
  - Lack of stringent security measures at the reseller level
  - Over-reliance on the trustworthiness of third-party resellers

DigiNotar Case

- In 2011, DigiNotar's systems were breached by attackers
- Fraudulent certificates were issued, including for Google
- Attackers targeted Iranian users to intercept Gmail communications
  - Enabled large-scale surveillance and data theft
- Possible consequences:
  - Massive privacy violations for affected users
  - Loss of trust in DigiNotar, leading to its bankruptcy
  - Undermining of the PKI ecosystem's credibility
- Why these consequences were possible:
  - Weak internal security controls at DigiNotar
  - Failure to detect and respond to the breach in a timely manner
  - Lack of transparency in notifying affected parties