TALENTO TECH

REGIÓN 3
CAUCA - NARIÑO
LESSON 3 -UNIT 2

TIC

Universidad Tecnológica de Pereira

faceIT

LESSON 3: Reading: Public-Key Certificates

What is a Public-Key Certificate?

A public-key certificate is a digital document issued by a Certificate Authority (CA) to authenticate an entity's identity and link it to a public key. The certificate contains important fields such as the serial number, the entity's name, the issuer's name, the validity period, and the public key information.

Purpose

Public-key certificates ensure secure communication by verifying the sender's identity and protecting online transactions from unauthorized access. They help maintain cybersecurity and streamline access management.

How They Work

Public-key certificates use asymmetric encryption, which involves a public key (accessible to everyone) and a private key (kept secret). The private key enables the owner to sign documents and prove their identity, fostering trust in digital interactions.

Core components of public key infrastructure

A PKI generally consists of the following elements:

- **Digital certificate**—also known as a public key certificate, this PKI component cryptographically links a public key with the entity that owns it.
- **Certificate authority (CA)**—the trusted party or entity that issues a digital security certificate.
- **Registration authority (RA)**—also known as a subordinate certificate authority, this component authenticates requests for a digital certificate and then forwards those requests to the certificate authority to fulfill them.
- **Certificate database and/or certificate store**—a database or other storage system that contains information about keys and digital certificates that have been issued.

Key Components of PKI

1. Public-Key Infrastructure (PKI): Secures communication using asymmetric encryption.
2. Certificate Authority (CA): Issues and validates certificates.
3. Registration Authority (RA): Verifies the entity requesting a certificate.
4. Certificate Database: Stores public certificates for validation purposes.

Types of Certificates

- **Domain Validation (DV):** Basic, quick to issue, and affordable.
- **Organization Validation (OV):** Verifies organizations and their root CA.
- **Individual Validation (IV):** Used for personal identity, often for email.
- **Extended Validation (EV):** Requires rigorous vetting for enhanced trust.
- **Client Certificates:** Authenticate individual users, not devices.
- **Email Certificates:** Secure email communication.
- **EMV Certificates:** Secure transactions using chip-enabled payment cards.
- **Code-Signing Certificates:** Ensure software authenticity and integrity.

Certificate Hierarchies

1. Root Certificates: The highest-level certificates that sign others.
2. Intermediate Certificates: Bridge root and end-user certificates.
3. Leaf Certificates: Used for specific purposes like SSL/TLS or email signing.
4. Self-Signed Certificates: Signed by their own public key, offering limited trust.

Advantages and Disadvantages

Advantages:

- Enable secure authentication.
- Protect against man-in-the-middle attacks.
- Widely supported and efficient in issuance.

Disadvantages:

- Lack of control if encryption keys are compromised.
- Risk of fraudulent certificates without warnings.

Public-key certificates remain a cornerstone of online security, ensuring identity verification and secure communication. Despite some risks, their benefits make them essential in today's digital landscape.