Cryptography

Madiba Hudson-Quansah

Contents

Chapter 1

Public Key Infrastructure

Definition 1.0.1: Public Key Infrastructure (PKI)

The systems the brings cryptography into real world use. Uses certificates, trusted authorities and public key cryptography to securely identify entities on a network.

PKI is the integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely over insecure networks like the internet using public key cryptography.

PKI solves the problem of **trust** in public key cryptography by using a **trusted third party** called a **Certificate Authority (CA)** to verify the identity of entities and issue digital certificates that bind public keys to those identities.

PKI protections information assets in all forms:

Authentication Validate

Integrity

Confidentiality

Authorization

Non-Repudation

1.1 Components of PKI

Certificate Authority (CA) :

- Trusted third party that issues digital certificates

Registration Authority (RA)
- Handles certification functions in collaboration with a CA, verifying registration information, generating end-user keys, and validating and revoking user certificates.

Digital Certificate (X.509)
- Owner's public key
- Owner's identify information
- Digital signature of the CA
- Validity period
- Certificate serial number

Certificate Store/Repository - Central location where certificates and CRLS (Certificate Revocation Lists) are stored and managed.

Certificate Revocation List (CRL) - A list of certificates that have been revoked before their expiration date.

Management Protocols

- Manages the Lifecycle of keys and certificates
- Organizes and manages communicators among CAs, RAs, and end users, while ensuring secure transmission of certificates and related information.

Policies and Procedures

- Assists an organization in the application and management of certificates in the formalization of legal liabilities and limitations and in business use.