Advanced PKI Cryptography Concepts

Dr. Dwayne Hodges, USA, (Ret.)

CISSP, CCISO, CEH, CNDA, ECES, SEC+ ITIL

Advanced PKI Cryptography Concepts

- Goals of Cryptography (Cryptosystem)
  - Confidentiality
  - Integrity
  - Availability
  - Non-Repudiation

Advanced PKI Cryptography Concepts

Public Key Infrastructure (PKI)

- A framework for managing public keys keys and certificates
- Provides a standard for key generation, authentication, distribution, and storage
- Establishes who is responsible for authenticating the identity of the owners of the digital certificates
- Follows the X.509v3 standard

Advanced PKI Cryptography Concepts

Digital Signatures

- X.509v3
  - International Telecommunication Union (ITU) standard for defining digital certificates
  - Defines the formats and fields for public keys
  - Defines procedures for distributing public keys
    - Current standard: X.509 v.3
- Public-Key Cryptography Standards (PKCS)
- **p12- PKCS#12, others out -**
  - Developed by RSA Laboratories

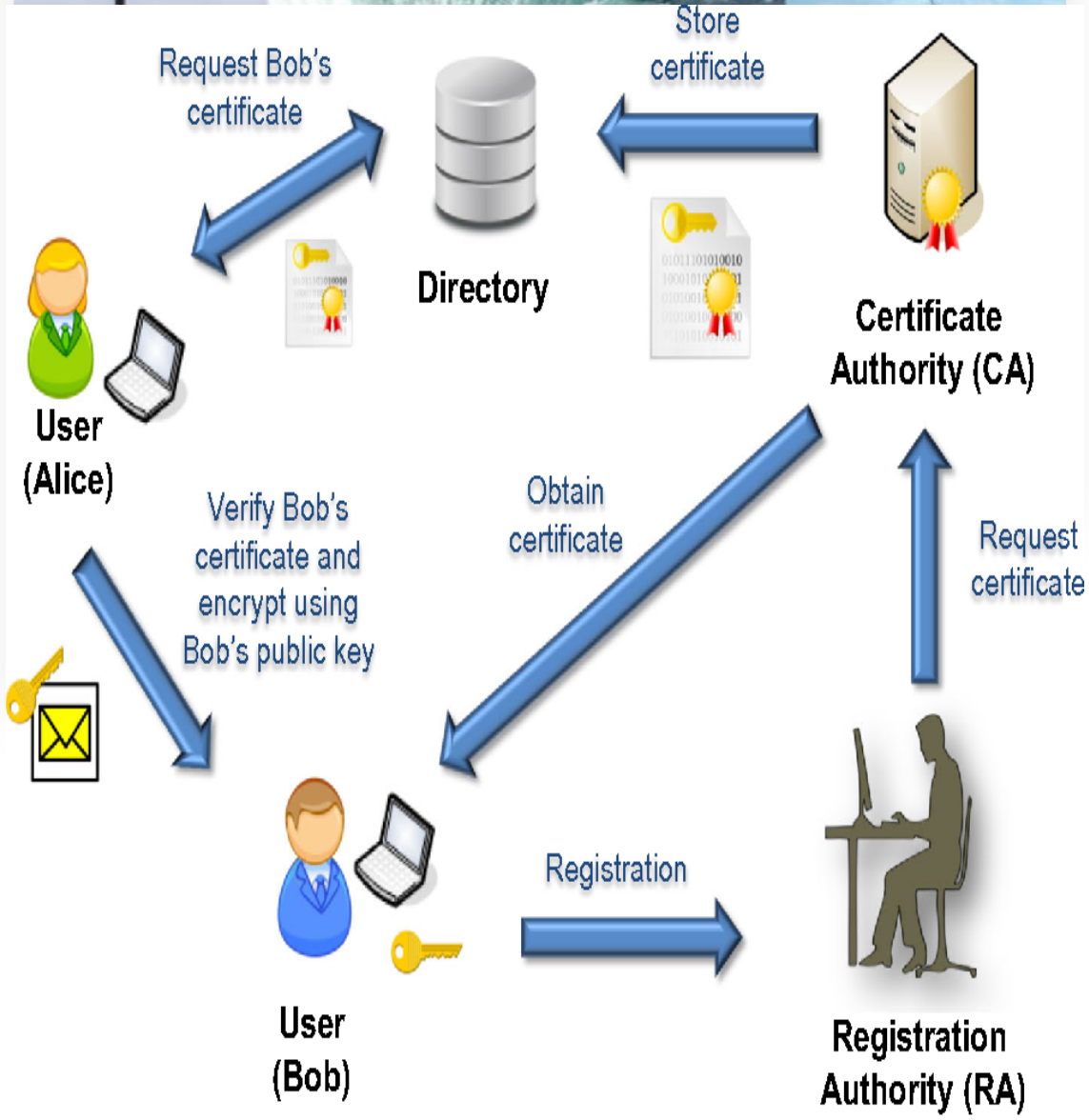
Advanced PKI Cryptography Concepts

Certificate Management (X.509v3)

- Enables the authentication of the parties involved in a secure transition
- A typical certificate contains the following:
  - The certificates issuer's name
  - Valid from date / to date
  - The owner of the certificate (subject)
  - The subject's public key
  - Time stamp
  - The certificates issuer's digital signature

Advanced PKI Cryptography Concepts

- **Class 1- Individuals, emails**
- **Class 2- organizations**
- **Class 3- software, servers**
- **Class 4- online business transactions**
- **Class 5- private, government**



Advanced PKI Cryptography Concepts

Certificate Authority (CA)

- Organization responsible for issuing, storing, revoking, and distributing certificates
- Authenticates the certificates it issues by signing them with their private key

- Registration Authority (RA)
  - Middleman between subscribers and CA
  - Can distribute keys, accept registrations for the CA, and validate identities
  - RA does not issue certificates on their own

Advanced PKI Cryptography Concepts

Certificate Policy

- Dictates the circumstances in which a certificate can be used
- Protects the CA from claims of loss if the certificate is misused
- Should identify the user's community, names of the CA and RA, and the object identifier

Advanced PKI
Cryptography Concepts

Certificate Pinning – the process of associating x509v3 certificate or public key

or

Certificate Revocation List (CRL)

- Identifies revoked certificates
- Expired certificates are not on the CRL

Online Certificate Status Protocol (OCSP)

- Checks for revoked certificates
- OCSP queries a CA or RA that maintains a list of expired certificates
- Server sends a response with a status of valid, suspended, or revoked

Advanced PKI Cryptography Concepts

Certificate Revocation

- Certificates are revoked due to:
  - compromised
  - Key theft
  - Loss
  - Illegal activity
  - Significant changes in the organization (change in name, ISP, or key personnel)

Not revoked due to normal expiration

Advanced PKI Cryptography Concepts

- Certificate Server
  - A central repository for storing certificates
  - Allows administrators to set policies in one location and to centrally manage all users' certificates
- Certificate Expiration
  - If a certificate expires, a new certificate must be issued
  - Expired certificates are NOT added to the CRL

Advanced PKI Cryptography Concepts

Certificate Suspension

- Certificates can be suspended
- Ensures the key is unusable for a period of time
- Suspend rather than expire certificates to make them temporarily invalid
  - Particularly when you anticipate that the certificate holder will return to their normal course of duties

Advanced PKI Cryptography Concepts

Trust Models

Trust models explain how users can establish a certificate's validity

Common models:

- Single-Authority Trust
  - Single CA, everyone is configured with a public key, CA signs all pubic keys, many Ras trusted my CA
- Hierarchical Trust
  - All nodes trust the CA- the upside-down tree
- Bridge Trust
  - CA-CA,
    - Dep- Dep
- Web of Trust
  - Applications (PGP)

Advanced PKI Cryptography Concepts

Certificate Destruction and Lifecycle

- Keys to the Kingdom
- Establish policies for destroying old keys
- When a key or certificate is no longer useful, destroy and remove from the system
- When destroyed, notify the CA so the CRL and OCSP servers can be updated
- Deregistration should occur when a key is destroyed, especially if the key owner no longer exists (such as a company out of business)

Advanced PKI Cryptography Concepts

- Primary role of CA is to digitally sign all user certificates with the CAs private key
- CA manages all public public keys and DS
- CA distribute certificates and public keys
- Certificate contains user's public key
- CA verifies users identifies, bounds users to certificates
- CA provides trust between multiple users
- CA can be public or private
- RA handles verification and acts as proxy, receives request
- CRL is a list of revoked certificates
- OCSP- real time protocol for verifying certificates
- X509v3, most widely used standard, contains public key signed by CA (trusted 3rd party)
- CP – set of rues that define hoe a certificate may be used
- Digital certificate - document that contains a public key and some other information used for verification
- Digital signature (DS)–encrypted message with a private key
- DS is verified with sender's public key