

# PKI - CA - Digital Signature

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: pki\_ca\_ds.pdf*
- ❖ *GNU Free Documentation License*
- ❖ *Version 1.00, 2005-05-27*
- ❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*
- ❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

## ❖ PKI / CA

- **Secure a wide range of communications channels.**
- **You can implement certificate-based security**
- **By obtaining certificates from a public Certificate Authority (CA)**
- **Or by establishing your own CA.**
- **First step in the process is setting up PKI**
- **PKI**
  - **Up link and down link refer to the two transmission channels between the CRL**
  - **PKI is an ISO authentication framework that uses public key and the X.509 standard**
  - **PKI is implemented through a trust model (CA hierarchy)**
  - **Consists of**
    - Programs
    - Data format
    - Procedures
    - Communication protocols
    - Security policies
    - Public key mechanisms
  - **PKI integrates**
    - Digital certificates
    - Public-key cryptography
    - Certificate authorities
  - **PKI - provides**
    - Authentication
    - Confidentiality
    - Nonrepudiation
    - Integrity
    - Access Control
  - **PKI is made of different parts**
    - Digital certificate
      - ◆ Electronic documents that bind the entity's public key
      - ◆ A signed statement from a trusted party
      - ◆ Verify that an entity is who it claims to be
      - ◆ They are composed of:
        - Sender Public Key
        - Sender Name
        - Expiration Date of the Sender Public Key
        - Name of the Certificate Issuer
        - Serial Number of the Certificate
        - Digital Signature of the Issuer

- Certificate Authority (CA)
    - ◆ Acts as a notary to bind the key to the person
    - ◆ Maintains and issues public key certificates
    - ◆ Responsible for issuing digital certificates
    - ◆ CA Hierarchy
      - The highest certification authority is called the root CA.
      - Root CAs can be designated either private or public.
      - Private root CA is created by a company itself
      - Public root CA is created by a third-party
      - Subordinate CA
        - Also issue certificates
        - Responsible for
          - Renewal
          - Suspension
          - Revocation
      - An organization may create as many subordinate CA's
      - Certificate policy (CP)
        - Is a security policy
        - Determines what information a DS will contain
        - Determines what the requirements are to obtain a DS
        - The specifications for the information in the certificate
        - Developed by representatives from the entire company
        - Considerations
          - How will users be authenticated to the CA?
          - What are the legal implications if the CA is compromised?
          - What is the certificate going to be used for?
          - How will the user's private key be stored?
          - What is the user responsible for?
          - Can the user's private key be exported?
          - What are the requirements to renew a certificate?
          - How long will the certificate lifetime be?
          - What type of crypto will the certificate use?
          - What will be the length of the public and private key pair?
      - After the CP creation, the CA software is configured to implement the (CP)
      - Separate certificate practice statement (CPS) is developed
      - CPS specifies how a particular CA will manage its certificates
    - ◆ The Certificate Life Cycle.
      - Issuance
      - Revocation
      - Expiration
      - Renewal
      - The longer the life cycle is, the less administrative overhead
      - This could pose a higher security risk
- Registration authority (RA)
  - ◆ Performs the certification registration duties.
  - ◆ Responsible for verifying users identity
  - ◆ Approve or deny requests for digital certificates.
- Certificate repository
  - ◆ The database that contains the digital certificates.
- Certificate management system
  - ◆ Software tools to perform the day-to-day functions of the PKI.
- Certificate revocation list (CRL)

- ♦ A list of every certificate that has been revoked for one reason or another
  - ♦ This list is maintained periodically
- **In (PKI) certificates enhance:**
  - A.) Nonrepudiation
  - B.) Confidentiality
  - C.) Message integrity
  - The use of certificates does not assure availability.
- **A source could post a public key under the name of another individual**
- **Digital certificates counter this attack, a certificate can bind individuals to their key**

## ❖ **Digital signature (DSs)**

- **Is the technique of appending a string of characters to an electronic message in order to authenticate the sender**
- **A Methode to let the receiver of the message prove the source and integrity**
- **Are an authentication tool to verify a messages origin and a sender's identity.**
- **It is created through the use of a hash function and a private signing function**
- **A digital signature is an ENCRYPTED HASH value**
- **The act of signing just means that the value was encrypted with a private key**
- **The sender private key is used to create a digital signature**
- **Encrypting a signature, data is always signed using the signer's private key**
- **If the receiver wants to verify the signer he Use the public key of the signer**
- **Two components of a DS are**
  - The original message
  - The sender private key
- **These signature are based on public key encryption (Asymmetric)**
- **Because it is Asymmetric it helps**
  - **Ensure integrity**
    - The hashing function
  - **Ensure confidentiality**
- **Purpose of Digital Signatures**
  - **The hashing function ensures the integrity**
  - **The signing of the hash value provides authentication and non-repudiation**
  - **To Detect unauthorized modifications and to authenticate identity and non-repudiation.**
  - **Generates block of data smaller than the original data**
  - **Binds message to individual**
  - **Can't be forged**
  - **Block of data attached to message (document, file, record, etc)**
  - **Hashing algorithm generates a message digest of 160 bits**
  - **Message digest should be calculated using all of original files data**
- **How does it work**
  - **Original text is sent through a hashing algorithm**

- Resulting a string of hexadecimal (Message Digest)
- **The message digest is encrypted with the sender private key**
  - Resulting in the Digital Signature
- **The sender encrypt the digital signature with a New Random Key**
- **The sender encrypt the New Random Key with the recipient public key**
  - Resulting in a Digital Envelope
- **The encrypted message, encrypted DS, and Digital Envelope are sent to the recipient**
- **The original message is assembled using a Cyclic Redundancy Check**

#### ➤ **DSA**

- **Digital signature algorithm (DSA)**
- **Is an asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers.**
- **This algorithm uses a private key to sign a message and a public key to verify the signature.**
- **It is a standard proposed by the U.S. Government.**
- **DSA is used to Digitally sign the message**

#### ➤ **Operation of the Digital Signature Standard**

#### ➤ **Benefits of the Digital Signature Standard**

#### ➤ **Notes about message**

- **A message can be ENCRYPTED which provides CONFIDENTIALITY**
- **A message can be HASHED which provides INTEGRITY**
- **A message can be DIGITALLY SIGNED which provides AUTHENTICATION & INTEGRITY**
- **A message can be ENCRYPTED and DIGITALLY SIGNED which provides CONFIDENTIALITY, AUTHENTICATION, and INTEGRITY**

### ❖ **One-way function $Y=F(X)$**

- **Is a mathematical function that is easier to compute in one direction than in the opposite direction**
- **Easy to compute Y if X is given**
- **VERY difficult to derive X given Y**
- **One-way function is like multiplying two large prime numbers**
- **Provide confidentiality and authentication**
- **Trapdoor**
  - **One way hash function to be useful in the context of public key, it should have a trapdoor**
  - **Trapdoor is a secret mechanism that enables you to easily accomplish the reverse of the one way function**
- **An analogy when you drop a glass on the floor**
- **Many public key encryption algorithms are based on the difficulty of factoring large numbers that are the product of two large prime numbers**
- **Public key cryptography is based on TRAPDOOR one-way functions**

### ❖ **Harden a Certificate Authority**

- **Take the root CA offline, after the configuration**
- **Only authorized entities can obtain certificates.**

- **Place all CA servers behind a firewall.**
- **Physically secure the CAs.**
- **Use longer key lengths for better security**
- **Limit administrative access to the CAs.**
- **Back up the certificate database regularly.**
- **Back up the entire CA server regularly.**
- **Keep current with security patches and fixes**