

# Cryptography Managing Certificates

❖ *DigitalSherlock.com | SafeHack.com*

❖ *Date: 2005/05/27*

❖ *Document Name: cryptography\_managing\_certificates.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.*

## ❖ **Enroll certificates for entities.**

- **Using certificates is a process that has several stages.**
- **The first stage is enrolling and installing certificates**
- **Certificate enrollment depends on the level of security the CA requires**
- **The exact process is determined by the certificate policy (CP)**
- **Steps**
  - **Entity submits request for certificate.**
  - **User authenticated by the RA.**
  - **Policy applied to request.**
  - **Request sent to CA.**
  - **CA issues certificate.**
  - **User is notified certificate is complete.**
- **Thousands of Certificates to Enroll**

## ❖ **Secure network traffic using certificates.**

- **Once an entity has a certificate enrolled**
- **You can use the certificate to secure network**
- **Setting up the security is the next step in the process**
- **To secure a Windows 2000 Web**

## ❖ **Renew certificates.**

- **Your first concern is renewing existing certificates**
- **Certificates are designed to expire at regular intervals**
- **Renew a CA certificate in Windows 2000**

## ❖ **Revoke certificates.**

- **A Certificate Revocation List (CRL)**
- **List of certificates that were revoked before the expiration date**
- **When the CRL is published the users know that the certificate is revoked**
- **Reasons to revoke a certificate**
  - **Certificate owner's private key has been compromised or lost.**
  - **The certificate was obtained by fraudulent means.**
  - **The entity is no longer trustworthy**
- **Certificate revocation permanently invalidates a given certificate.**
- **Destroying Certificate Files after you revoke it**
- **Some Unix certificate server support certificate suspension**
- **Which enables you to temporarily invalidate a certificate**

- **Certificate suspension is not supported on Windows 2000**
- **Revoke a certificate in Windows 2000**

### ❖ **Back up certificates and private keys.**

- **Keys are occasionally damaged or lost.**
- **You need to have backup procedures for certificates and keys**
- **Back up user certificates and private keys in Windows 2000**

### ❖ **Restore certificates and private keys.**

- **Certificates and private keys can get lost or destroyed,**
- **Restoring the certificate from the backup is important**
- **Private Key Replacement**
  - **1. Recover the private key.**
  - **2. Decrypt any encrypted data.**
  - **3. Destroy the original private key.**
  - **4. Obtain a new key pair.**
  - **5. Re-encrypt the data.**
- **Private Key Restoration**
  - **A private key can become unavailable for several reasons**
  - **To recover the data, you must first restore the private key**
  - **2 methods to restore a lost private key:**
    - **Key escrow**
    - **Restore from backup**
  - **M of N Control**
  - **Procedure for Windows 2000**