

filename:comptia-secplussy0601-2-8-1-certificates

Showname: Security+ \ (SY0-601\)

Topic: Cryptography

Episode: Certificates

\*Given a scenario, implement public key infrastructure.\*

Description: In this episode, the viewer will learn how to identify different types of certificates that are used for a variety of reasons such as code signing, email as well as user and machine authentication and more. The viewer will also see how to determine the certificate format basic on the use case such as exporting the private key, format requirements and email.

-----

- \* Root and Sub CA Certs
  - + Self-signed
- \* Machine Certificate
  - + Servers
  - + Client Machines
  - + Network Devices
- \* User Certificates
  - + Email
  - + Disk Encryption
  - + Identity
- \* S/MIME
- \* Code Signing Certificates
- \* Wildcard Certificates
  - + \*.google.com
- \* Validation Certificates
  - + DV
  - + OV
  - + EV
  - + IV
- \* Certificate Format
  - + .der
  - + .pem
  - + PKCS#7
  - + PKCS#12

-----

- \* Demo - Show the RootCA and self-signed
- \* Demo - Initiate a CSR with MMC and Certificate Snap-in
- \* Demo - Local Machine/Local User Certificate Snap-ins
- \* Demo - Show available certificates, discuss properties
- \* Demo - Start installation of NotePad++ \ (code signing\)
- \* Demo - start the Certificate Export Wizard (Formats)
- \* Demo - start without private key - show formats
- \* Demo - Show with private key formats