filename:comptia-secplussy0601-2-5-pki_concepts
Showname: Security+ \(SY0-601\)
Topic: Cryptography
Episode: PKI Concepts
Given a scenario, implement public key infrastructure
Description: In this episode, the viewer will identify the critical components of public key infrastructure such as certificate authorities (CAs), intermediate and root CAs, online vs. offline CA, registration authorities, OCSP, certificate revocation lists and more.

---

* Installing ADCS (Root)
    + Enterprise vs. Standalone
    + Roots vs. SubCAs
    + CSPs
    + Key length \(longer=stronger/cpu intensive,shorter=weaker\)
    + Hashing Algorithm
    + Common Name (part of the DN, typically FQDN or server's hostname/domain and must match, part of X.509 standard)
    + Validaty Period
        - Roots longer
        - Subs Shorte
* Installing ADCS
    + Mention we are creating the sub (show cert chain for ITProTV\)
    + When installing we will create \(through the wizard\) a CSR (encoded text given to the RootCA\)
    + Mention additional roles
        - Online Responder \(OCSP\)

- NDES \(SDEP\)
- Certificate Web Enrollment

+ Enterprise vs. Standalone
+ Root vs. Sub
+ Key Length \(shorter for the intermediate\)
+ Create CSR
+ Finish install \(note cert install warning\)
+ From MBRSRV browse to MBRSRV2 via file explore
+ Copy cert req file andopen with Notepad.exe
+ Most cert signing requests are Base-64 encoded PEM format \(more about cert types in a later format\)
+ Use CertAuth to issue certificate
+ Show Cert, mention revoking and show CRL
+ Switch to MBRSRV2, open CertAuth
+ Start CA Service
+ Install certificate on MBRSRV2
+ Show CA Service Active
+ Logout as admin/login as wbryan
+ run mmc.exe then Crtl+M >> add Certificates
+ Generate CSR
+ Logout/ login as admin
+ Launch CA show cert and cert chain