CompTIA Security + 6.0 Cryptography and PKI

Filename: comptia-secplussy0501-6-4-public_key_infrastructure
Title: Public Key Infrastructure
Subtitle: CompTIA Security+ (SY0-501)

6.4 Public Key Infrastructure

- 6.4 Given a scenario, implement public key infrastructure.
  - Components
    - Public key
    - Private key
    - Certificates
      - Users
      - Machines/Computers
      - Network Devices
      - SANs
      - Applications/Code Signing (show npp install on Windows 10 w/Extended Key usage)
      - Email
      - Certificates require CSR
      - Object identifiers (OID)
      - Show key usage on Win10 certs >mmc.exe > certificates >local machine > Trusted Root Authorities > Select > Microsofts Root Authority > Explain General Tab > Certificate purposes
    - CA
      - Root CA (Show local certifiate store)
        - Offline CA
        - Self-signed (Show Google)
        - Root Certificates \
    - Intermediate CA
      - Subordinate CAs
      - Issuing CAs
    - Trust Model
  - Components for Validation
    - Chain Validation
    - CRL(Show local computer cert and look in Intermesiate Certification Authority >Ceritifcation Revocation List)
    - OCSP
    - OCSP Stapling
  - Additional Concepts
    - Pinning- Ensuring that a single certificate is trusted
    - Key escrow
    - Wildcard
  - Types of certificates
    - SAN
    - Code signing (show npp install on Windows 10 w/Extended Key usage)
    - Self-signed (RDP from Win10 to SRV01)
    - Machine/computer (Show local certificate store)
    - Email (S/MIME)
    - User (Show Local Cerficate store)
    - Root(Show Local Cerficate store, Google chain)
  - Validation Methods
    - Domain validation(Verify's a domain belongs to the trusted company)
    - Organizational Validation (verifies the actual business that is using the certificate)
    - Extended validation (provides the highest level of encryptions, will include the business name in the browser)(www.SSL.com = EV CA)\
      - Signed Copy of EV Subscriber agreement
      - Signed Copy of EV Authorization Form
      - Letter from CPA
      - A letter from a Latin Notery
  - Certificate formats
    - DER
    - PEM
    - PFX
    - CER
    - P12
    - P7B