3.9

Monday, September 25, 2023 3:20 PM

machine certificates

PKCS #7 = P7B

.P12 and .PFX for private and pub

certification path = cert chaining = chain of trust

the certs for diff servers need to be same

CA hierarchy

- root = top
- subordinate = intermediate
- issuing CAs

Email certificates sign and encrypt emails

Server/computer certificates for hardware

Private vs public root certs

public use chain of trust

private orgs must load emp pc's web browser w/ internal certs

Subject Alternative name SAN = diff name

Wildcard = same name

pinning - ensure it is inspecting proper cert when client inspects cert prevents on-path

extended validation - more rigorous
check on subject's legal id
and control over domain

error in SAN = "does not support *"
extension field on web server
cert

X.509 cert standard & format

domain validation - proving ownership
of domain
may be proved via email
highly vuln

Encrypt emails w/ S/MIME or PGP

DER = binary

CER = ASCII

PEM = Base64

- .key
- .cert
- .cer

HTTP public key pinning HPKP

root CA must be powered on when adding subordinate CA to hierarchy

online CA sign, publish CRL, and other cert manage tasks

Common access card CAC - smart card for cert-based auth for cert-based auth

Common name CN - used to be used to id FQDN but is deprecated