COURSE: SECURITY+ SY0-401

MODULE 6: CRYPTOGRAPHY

Overview

- Given a scenario, use appropriate PKI, certificate management and associated components

Public Key Infrastructure

PKI is comprised of several standards and protocols. These standards and protocols are necessary to allow for interoperability among security products offered by different vendors. Keep in mind, for instance, that digital certificates may be issued by different trusted authorities; therefore, a common language or protocol must exist

Email	Secure Electronic Commerce	VPN
S/MIME	SSL TLS	IPsec PPTP
PKIX PKCS X.509		

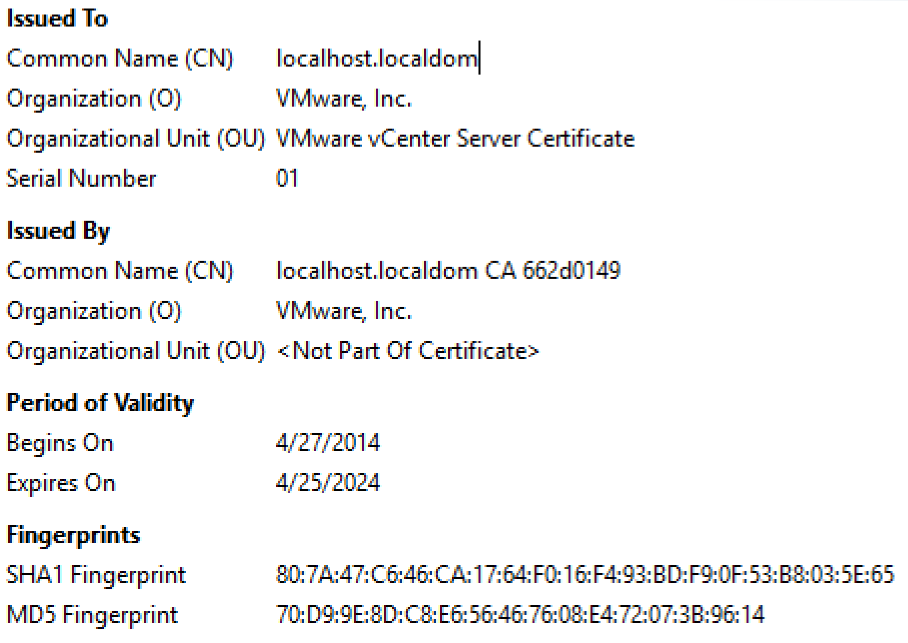
Public Key Infrastructure

PKI X.509

IETF working group created standards for X.509 PKI. X.509 is an International Telecommunications Union (ITU) recommendation and is implemented as a de-facto standard.

X.509 defines a framework for authentication services by a directory.

- Version
- Serial Number
- Signature Algorithm Identifier
- Issuer
- Validity Period
- Subject Name
- Subject Public Key Information



Issued To	
Common Name (CN)	localhost.localdom
Organization (O)	VMware, Inc.
Organizational Unit (OU)	VMware vCenter Server Certificate
Serial Number	01
Issued By	
Common Name (CN)	localhost.localdom CA 662d0149
Organization (O)	VMware, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>
Period of Validity	
Begins On	4/27/2014
Expires On	4/25/2024
Fingerprints	
SHA1 Fingerprint	80:7A:47:C6:46:CA:17:64:F0:16:F4:93:BD:F9:0F:53:B8:03:5E:65
MD5 Fingerprint	70:D9:9E:8D:C8:E6:56:46:76:08:E4:72:07:3B:96:14

Certificate Authority

Certificate authorities (CAs) are trusted entities and are an important concept within PKI. Aside from the third-party CAs, such as VeriSign (now part of Symantec Corp.), an organization may establish its own CA, typically to be used only within the organization. The CA’s job is to issue certificates, to verify the holder of a digital certificate, and to ensure that holders of certificates are who they claim to be. A common analogy used is to compare a CA to a passport-issuing authority

Public Key Infrastructure

- Certificate authorities and digital certificates
  - CA
  - CRLs
  - OCSP
  - CSR
- PKI
- Recovery agent
- Public key
- Private key
- Registration
- Key escrow
- Trust models

Public Key Infrastructure

Registration authorities (RAs) provide authentication to the CA as to the validity of a client's certificate request; in addition, the RA serves as an aggregator of information. A user, for example, contacts an RA, which in turn verifies the user's identity before issuing the request of the CA to go ahead with issuance of a digital certificate.

A digital certificate is a digitally signed block of data that allows public key cryptography to be used for identification purposes. CAs issue these certificates, which are signed using the CA's private key. Most certificates are based on the X.509 standard. Although most certificates follow the X.509 version 3 hierarchical PKI standard, the PGP key system uses its own certificate format

Public Key Infrastructure

Key Escrow: *Escrow* refers to a trusted third party or broker. A deposit on a new home, for example or a third-party account used to fulfill property tax obligations are examples of escrow. A key escrow then is similar but is specifically used to mitigate key loss or protect entities to ensure agreed upon obligations are fulfilled.

Exportation: When digital certificates are issued, they receive an expiration date. This validity period is indicated in a specific field within the certificate. Many certificates are set to expire after one year; however, the time period may be shorter or longer depending on specific needs. Open a certificate from within your browser while visiting a secured site (in most web browsers, select the padlock icon from the browser's status bar) and notice the "Valid to" and "Valid from" fields within the certificate

Public Key Infrastructure

Suspension: Certificate suspension occurs when a certificate is under investigation to determine whether it should be revoked. This mechanism allows a certificate to stay in place, but it is not valid for any type of use.

Recovery: Key recovery is the process of using a recovery agent to restore a key pair from a backup and re-create a digital certificate using the recovered keys. Unlike in the case of a key compromise, this should be done only if the key pair becomes corrupted but they are still considered valid and trusted. Although it is beneficial to back up an individual user's key pair, it is even more important to back up the CA's keys in a secure location for business continuity and recovery purposes.

THANK YOU