Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/8/2022 8:13:05 pm • Time spent: 01:53

Score: 80% Passing Score: 80%

Question 1: ✓ Correct

An SSL client has determined that the certificate authority (CA) issuing a server's certificate is on its list of trusted CAs. What is the next step in verifying the server's identity?

○ The master secret is generated from common key code.

○ The post-master secret must initiate subsequent communication.

➡ ● The CA's public key must validate the CA's digital signature on the server certificate.

○ The domain on the server certificate must match the CA's domain name.

EXPLANATION

Once an SSL client has identified a CA as trusted, it uses the CA's public key to validate the CA's digital signature on the server certificate. If the digital signature can be verified, the client accepts the server certificate as a valid certificate issued by a trusted CA.

SSL clients verify a server's identity using the following steps:

1. The client checks the server's certificate validity period. The authentication process stops if the current date and time fall outside of the validity period.
2. The client verifies that the issuing certificate authority is on its list of trusted CAs.
3. The client uses the CA's public key to validate the CA's digital signature on the server certificate. If the digital signature can be verified, the client accepts the server certificate as a valid certificate issued by a trusted CA.
4. To protect against man-in-the-middle attacks, the client compares the actual DNS name of the server to the DNS name on the certificate.

REFERENCES

7.5.2 Public Key Infrastructure Facts

q_cryt_pki_ca_02_secp7.question.fex

Question 2: ✓ Correct

Which of the following would require that a certificate be placed on the CRL?

- ○ The encryption key algorithm is revealed.
- ➡ ● The private key is compromised.
- ○ The certificate validity period is exceeded.
- ○ The signature key size is revealed.

EXPLANATION

Certificates are published to the Certificate Revocation List (CRL) when a condition compromises the integrity of the certificate. If the private key is compromised (discovered), the certificate is no longer proof of identity.

Certificates do not need to be placed on the CRL if their validity period expires. In this case, the certificate simply expires. Knowing the signature key size or the encryption key algorithm does not compromise the integrity of the certificate.

REFERENCES

7.5.2 Public Key Infrastructure Facts

q_cryt_pki_crl_03_secp7.question.fex

Question 3: ✓ Correct

Which technology was developed to help improve the efficiency and reliability of checking the validity status of certificates in large, complex environments?

- ○ Key escrow
- ○ Certificate Revocation List
- ○ Private key recovery
- ➡ ◉ Online Certificate Status Protocol

EXPLANATION

Online Certificate Status Protocol (OCSP) is the technology developed to improve the efficiency and reliability of checking the validity status of certificates in large, complex environments. OCSP allows clients to query a CA or registration authority (RA) and quickly learn whether a certificate is valid or has been revoked.

OCSP is a significant improvement over the CRL mechanism. CRLs were static lists that were distributed periodically to CAs and RAs. However, CRLs were often out of date. Key escrow and private key recovery are not related to certificate status checking.

REFERENCES

7.5.2 Public Key Infrastructure Facts

q_cryt_pki_ocsp_secp7.question.fex

▼ **Question 4:** ✓ Correct

A PKI is an implementation for managing which type of encryption?

○ Steganography

○ Symmetric

➡ ● Asymmetric

○ Hashing

EXPLANATION

A public key infrastructure (PKI) is a hierarchy of computers that issue and manage certificates. Certificates use asymmetric encryption with a public and private key pair.

REFERENCES

7.5.2 Public Key Infrastructure Facts

q_cryt_pki_pki_02_secp7.question.fex

Question 5: ✕ Incorrect

To obtain a digital certificate and participate in a public key infrastructure (PKI), what must be submitted and where?

➡ ○ Identifying data and a certification request to the registration authority (RA)

○ Identifying data and a secret key request to the subordinate distribution authority (DA)

○ Identifying data with the 3DES block cipher to the hosting certificate authority (CA)

● ~~Identifying data with the MAC and IP addresses to the root certificate authority (CA)~~

EXPLANATION

The registration authority (RA) processes all requests for digital certificates. Registration and authentication requirements vary based on the class of certificate requested. Once the RA has successfully authenticated the requesting party, the request is forwarded to the certificate authority (CA) for certificate generation.

REFERENCES

7.5.2 Public Key Infrastructure Facts

q_cryt_pki_ra_02_secp7.question.fex

Question 6: ✕ Incorrect

In the certificate authority trust model known as a hierarchy, where does trust start?

○ Third-party CA

○ Issuing CA

➡ ○ Root CA

● ~~Registration authority~~

EXPLANATION

Trust starts at the Root CA in all trust models.

An Issuing CA can be a Root CA or a CA at any level below the root.

A third-party CA may be the source of trust, but even then, the trust starts at a Root CA located somewhere.

A registration authority (RA) is a limited-functionality CA where certificates are verified, but no new certificates can be issued.

REFERENCES

7.5.4 Certificate Types Facts

q_cert_types_ca_secp7.question.fex

Question 7: ✓ Correct

Which standard is most widely used for certificates?

- ○ SSL v.3.0
- ➡ ● X.509
- ○ HTTP 1.1
- ○ 802.1x

EXPLANATION

The standard for certificates that is most widely used is X.509. This standard defines the key elements that must exist within a certificate. This standard is used by public key infrastructure (PKI), SSL, IPsec, DES, and many other infrastructure components and technologies.

HTTP 1.1 is the latest version of the protocol used to transmit web resources from a web server to a web client. SSL v.3.0 uses certificates, but this is the standard for the secure session protocol for protecting web communications. 802.1x is a networking protocol that defines how to support Extensible Authentication Protocol (EAP) over a wired or wireless LAN.

REFERENCES

☰ 7.5.8 Extended Validation Facts

q_cryp_validation_x509_secp7.question.fex

Question 8: ✓ Correct

A private key has been stolen. Which action should you take to deal with this crisis?

○ Place the private key in escrow

○ Delete the public key

➡ ● Add the digital certificate to the CRL

○ Recover the private key from escrow

EXPLANATION

If a private key--a digital certificate or digital signature--is compromised (especially by theft), it should be added to the CRL. This prevents any future use of the key/certificate and prevents impersonation attacks.

There is no need to delete the public key because CRLs deal with any attempted use of the private key. The private key should have been placed in escrow at the beginning of its lifetime if key recovery was desired. In this situation, key recovery is not necessary.

REFERENCES

7.5.10 Certificate Concepts Facts

q_cert_concepts_crl_01_secp7.question.fex

Question 9: ✓ Correct

You are concerned that if a private key is lost, all documents encrypted with your private key will be inaccessible. Which service should you use to solve this problem?

○ CSP

○ RA

➡ ● Key escrow

○ OCSP

EXPLANATION

Key escrow backs up private keys to a third-party organization outside of the company. If the private key is lost, you can recover the key from escrow.

Online Certificate Status Protocol (OCSP) is a protocol used to check the status of an individual digital certificate to verify whether it is good or has been revoked. A Cryptographic Service Provider (CSP) resides on the client and generates the key pair. A registration authority (RA) verifies the information included in a certificate request.

REFERENCES

7.5.10 Certificate Concepts Facts

q_cert_concepts_escrow_02_secp7.question.fex

Question 10: ✓ Correct

Which of the following items are contained in a digital certificate? (Select two.)

- □ Root CA secret key
- ➡ ☑ Public key
- ➡ ☑ Validity period
- □ Private key

EXPLANATION

Digital certificates create a link between identities and public keys. A certificate contains the information necessary to identify the public key owner. Certificates include fields detailing the Issuing CA and the standards version used to generate the certificate, as well as a certificate serial number, all approved uses for the certificate, the certificate owner, the public key and algorithm, the validity period, and the algorithms used to digitally sign the certificate. Additional functionality and data may be added through the use of certificate extensions.

REFERENCES

7.5.10 Certificate Concepts Facts

q_cert_concepts_key_secp7.question.fex