WGU

Introduction-to-Cryptography

WGU Introduction to Cryptography HNO1

Questions & Answers (Demo)

Version: 4.1

Question: 1

(What is an alternative to using a Certificate Revocation List (CRL) with certificates?)

A. Privacy Enhanced Mail (PEM)

B. Online Certificate Status Protocol (OCSP)

C. Root Certificate Authority (CA)

D. Policy Certificate Authority (CA)

Answer: B

Explanation:

OCSP is the primary online alternative to CRLs for checking whether a certificate has been revoked. With a CRL, a relying party periodically downloads a list of revoked certificate serial numbers published by the issuing CA (or CRL distribution point). That approach can be bandwidth-heavy, introduces latency between revocation and client awareness, and can result in clients using stale revocation data if updates are infrequent. OCSP improves this by allowing a client (or a server on the client's behalf) to query an OCSP responder in near real time about the status of a specific certificate (good, revoked, or unknown). In practice, many TLS deployments use OCSP stapling, where the server periodically fetches a signed OCSP response from the CA's responder and "staples" it to the TLS handshake, reducing client-side network calls and improving privacy (the CA doesn't learn which site the client is visiting). Thus, OCSP provides a more timely, certificate-specific revocation status mechanism than CRLs while preserving the CA's signed assurance.

Question: 2

(A company wants to use certificates issued by a root CA to demonstrate to customers that it is a legitimate company being hosted by a cloud provider. Who needs to trust the root CA public key?)

A. The seller and the buyer

B. The cloud provider and the seller

C. The Federal Trade Commission and the cloud provider

D. The buyer and the Federal Trade Commission

Answer: A

Explanation:

In a public key infrastructure, trust in a certificate ultimately depends on the relying party's trust anchor set—typically the root CA certificates preinstalled in a customer's browser/OS trust store. For customers to accept the company's certificate as legitimate, the buyer (customer) must trust the root CA public key (or an intermediate chained to it) so they can validate the certificate chain and signatures. The seller (the company) also must trust and rely on the root CA public key to build and present a valid chain and to make operational decisions based on that CA's issuance and revocation mechanisms; practically, the seller selects a CA whose root is widely trusted by customers. The cloud provider's trust is not what makes the certificate valid to customers; the provider may terminate TLS or pass traffic through, but customer validation is based on the chain to a trusted root. Government agencies like the FTC are not part of the cryptographic trust path for TLS certificate validation. Therefore, among the given options, the correct pairing is the seller and the buyer, reflecting both the issuer selection/usage by the company and the relying-party validation by customers.

Question: 3

(Which operation can be performed on a certificate during the "Issued" stage?)

A. Creation

B. Key recovery

C. Distribution

D. Key archiving

Answer: C

Explanation:

The "Issued" stage in a certificate lifecycle indicates that the certificate has been generated and signed by the issuing CA and is now valid for use (subject to validity dates, policy constraints, and revocation status). At this point, the operational focus shifts from creating the certificate to making it available to the subject and relying parties. "Distribution" is the lifecycle activity most directly associated with an issued certificate: installing it on servers or endpoints, provisioning it into keystores, publishing it to directories if required, and ensuring the chain (intermediates) is accessible for validation. By contrast, "Creation" is earlier in the process (key generation, CSR creation, identity validation, issuance/signing). "Key recovery" and "key archiving" relate to private key management and escrow policies (often for encryption keys, not signing keys), and are governed by organizational policy and key management systems rather than the certificate's issued state itself. A certificate can be distributed after issuance regardless of whether any key escrow features exist. Therefore, the operation that fits the certificate's "Issued" stage best is distribution of the issued credential for operational use.

Question: 4

(Which authentication method allows a web service installed on a network operating system to prove its identity to a customer?)

A. One-way client authentication

B. One-way server authentication

C. Mutual authentication

D. End-to-end authentication

Answer: B

Explanation:

One-way server authentication is the standard model used by most TLS-enabled web services to prove the server's identity to a client. In this model, the server presents an X.509 certificate during the TLS handshake. The client validates the certificate chain to a trusted root CA, checks hostname binding (CN/SAN), validates validity dates, and may check revocation status. If validation succeeds, the client gains cryptographic assurance that it is communicating with the holder of the private key corresponding to the server certificate's public key, and that the certificate is issued to the expected domain/identity. This proves the server's identity to the customer without requiring the customer to present a certificate. Mutual authentication would require both client and server to authenticate each other using certificates (commonly in certain enterprise APIs), but the question asks specifically about the web service proving its identity to the customer, which is satisfied by server-only authentication. One-way client authentication is the opposite direction (client proves identity to server). "End-to-end authentication" is a broader concept and not the specific TLS identity proof mechanism described here. Thus, one-way server authentication is the correct choice.

Question: 5

(Which authentication method allows a customer to authenticate to a web service?)

A. One-way server authentication

B. End-to-end authentication

C. Mutual authentication

D. One-way client authentication

Answer: D

Explanation:

One-way client authentication is the method where the client (customer) proves its identity to the server (web service). In cryptographic terms, this is commonly implemented through client credentials such as client TLS certificates (mTLS from the server's perspective) or through authentication protocols layered over TLS (for example, signed tokens), but the defining direction is that the client is the party being authenticated. In a strict TLS certificate-authentication framing, client authentication occurs when the server requests a client certificate during the handshake and the client demonstrates possession of the corresponding private key (via signature in handshake messages). The server then validates the client certificate chain and authorization policy. One-way server authentication, by contrast, authenticates only the server to the client and does not identify the customer. Mutual authentication authenticates both sides simultaneously; while it includes client authentication, it is broader than what the question asks. "End-to-end authentication" describes assurance between endpoints across intermediaries, but it is not the specific "customer authenticates to service" method in certificate-based terminology. Therefore, the best answer is one-way client authentication.