DUMPSQUEEN

Fundamental SOA Security

SOA S90.18

Version Demo

Total Demo Questions: 10

Total Premium Questions: 98

Buy Premium PDF

QUESTION NO: 1

Which of the following are valid reasons for a certificate to be revoked:

A. The certificate was fraudulently obtained

B. The public key has been compromised

C. The private key has been compromised

D. The subject is no longer permitted to use the certificate

ANSWER: A C D

QUESTION NO: 2

A service that was previously using a shared identity store is now given its own dedicated identity store instead. What are the likely impacts (positive or negative) that will result from this change?

A. The service's autonomy is increased.

B. The operational responsibility is increased due to the need to keep the dedicated identity store in synch with a parent identity store.

C. The potential to apply the Service Abstraction principle is increased.

D. The service will no longer be dependent on a certificate authority.

ANSWER: A B

QUESTION NO: 3

Which of the following is not a hashing algorithm?

A. MD5

B. X.509

C. SHA-1

D. SHA-256

ANSWER: B

QUESTION NO: 4

Which of the following approaches represents a valid means of utilizing generic security logic?

A. When required, generic security logic can be embedded within a service. The close proximity to the service logic maximizes the chances that the security logic will be consistently executed without interference from attackers.

B. When required, generic security logic can be abstracted into a separate utility service. This allows for reuse.

C. When required, generic security logic can be abstracted into a service agent. This allows for reuse and the security logic can be executed in response to runtime events.

D. All of the above.

ANSWER: D

QUESTION NO: 5

The services in a service inventory have all been built with compatible security technologies and mechanisms. Now, security policies are being introduced for the first time. How can security policies become part of the service inventory and its services while adhering to the application of the Standardized Service Contract principle?

A. SAML is used to ensure that security policies are consistently enforced, thereby naturally complying to service contract standards.

B. Canonical XML is used to ensure that all security policies are based on canonical policy models.

C. Both SAML and Canonical XML are required to ensure that that Standardized Service Contract principle can be effectively applied.

D. None of the above

ANSWER: D

QUESTION NO: 6

A certificate authority is generally responsible for

A. authenticating the identity of an entity requesting a certificate

B. publishing information about revoked certificates

C. receiving notifications about the loss of private keys

D. signing certificates that bind a public key to authenticate identity information about the key holder

ANSWER: A B C D

QUESTION NO: 7

Which of the following industry standards enable non-repudiation?

A. XML-Encryption

B. XML-Signature

C. SAML

D. None of the above

ANSWER: B C

QUESTION NO: 8

A SAML assertion always contains:

A. the name of the issuer

B. a validity period

C. subject confirmation

D. signature

ANSWER: A B

QUESTION NO: 9

Service A is a utility service that has been designed to receive and send non-confidential messages. Service A provides access to a legacy application. Since the launch of Service

A. the overall usage volumes have increased beyond expectations. Upon a review of the access logs, it is discovered that most of the requests came from unauthorized service consumers. The application of the Direct Authentication and Data Confidentiality patterns will prevent this from happening in the future.

True

B. False

ANSWER: B

By applying the Data Origin Authentication pattern together with the Brokered Authentication pattern, you guarantee confidential message exchanges by a service consumer that needs to repeatedly authenticate itself with a set of services within the same service composition.

A. True

B. False

ANSWER: B