SOA S90-18A

Fundamental SOA Security

Version: 4.0

QUESTION NO: 1

Which of the following is not a hashing algorithm?

A. MD5
B. X.509
C. SHA-1
D. SHA-256

Answer: B
Explanation:

QUESTION NO: 2

The application of the Data Origin Authentication pattern only provides message integrity.

A. True
B. False

Answer: B
Explanation:

QUESTION NO: 3

Service A relies on a shared identity store. Service B has its own identity store. Service C also has its own identity store, but must also access the shared identity store used by Service A. Which service has the least reduction in autonomy as a result of its relationship with identity store mechanism(s)?

A. Service A
B. Service B
C. Service C
D. The autonomy of all services is affected equally

Answer: B
Explanation:

QUESTION NO: 4

The requirement to defer security related state data at runtime relates directly to the application of which service-orientation principle?

A. Service Loose Coupling
B. Service Autonomy
C. Service Abstraction
D. None of the above.

Answer: D
Explanation:

QUESTION NO: 5

The use of XML-Encryption supports the application of the Service Abstraction principle because the actual message remains hidden from the attacker.

A. True
B. False

Answer: B
Explanation:

QUESTION NO: 6

Service A sends a message to Service B which reads the values in the message header to determine whether to forward the message to Service C or Service D. Because of recent attacks on Services C and D, it has been decided to protect the body content of messages using some form of encryption. However, certain restrictions within the design of Service B will not permit it to be changed to support the encryption and decryption of messages. Only Services A, C and D can support message encryption and decryption. Which of the following approaches fulfill these security requirements without changing the role of Service B?

A. Transport-layer security is implemented between all services.
B. Message-layer security is implemented between all services.
C. Service B is removed. Instead, the routing logic is added to Service A.
D. None of the above

Answer: B
Explanation:

QUESTION NO: 7

The application of the Brokered Authentication pattern is best suited for a scenario whereby a service consumer does not need to re-authenticate itself with multiple services.

A. True
B. False

Answer: B
Explanation:

QUESTION NO: 8

The SAML and WS-Security industry standards can be applied to the same service composition architecture.

A. True
B. False

Answer: A
Explanation:

QUESTION NO: 9

As a requirement for accessing Service B, Service A needs to encrypt its request message. Service B decrypts the message, makes some changes, encrypts the message, and then forwards it to Service C. However, the message does not make it to Service C. Instead, a runtime error is raised by a service agent that does not support encryption. This service agent only requires access to the message header in order to route the message to the appropriate instance of Service C. It is therefore decided that the header part of the message will not be encrypted. Which of the following can be used to address this requirement?

A. certificate authority

B. SAML
C. non-repudiation
D. None of the above

Answer: D
Explanation:

QUESTION NO: 10

Digital signatures use encryption and hashing.

A. True
B. False

Answer: A
Explanation:

QUESTION NO: 11

The manager of an IT department decides to split up an existing enterprise service inventory into two domain service inventories. The public key used previously in the enterprise service inventory can continue to be used in one of the domain service inventories.

A. True
B. False

Answer: A
Explanation:

QUESTION NO: 12

A task service needs to access three entity services as part of a service composition. The task service needs to authenticate itself every time it accesses one of the three entity services. Because the task service must authenticate itself three times to complete its task, the current service composition design is considered inefficient. How can it be improved while continuing to fulfill the authentication requirements?

A. Increase the network bandwidth between the task service and the entity services.
B. Use a single sign-on mechanism.
C. Remove the authentication requirements within the service composition, thereby reducing the message size and making communication faster.
D. None of the above

Answer: B
Explanation:

QUESTION NO: 13

Service A and Service B belong to Organization A and Service C belongs to Organization B. Service A sends confidential messages to Service B, which forwards these messages to Service C. The message sent to Service C is intercepted by a load balancing service agent that determines which instance of Service C to route the message to. This entire message path needs to be encrypted in order to ensure message confidentiality from when the message is first sent by Service A until it is received by an instance of Service C. Organization A doesn't trust any intermediaries that may exist in between Service B and Service C and also doesn't want to share any keys with Organization B. Furthermore, there is a requirement to minimize any adverse effects on performance. Which of the following approaches fulfills these requirements?

A. Use message-layer security by adding symmetric encryption between Services A, B and C. This way,message content is not available to any intermediaries between Services B and C.
B. Because Service A and Service B exist within the same organizational boundary, use transport-layer security to provide message confidentiality. Use message-layer security via asymmetric encryption between Service B and Service C.
C. Use transport-layer security between Service B and Service C and use message-layer security via asymmetric encryptionbetween Service A and Service B. This way. all the services are secured while at the same time minimizing the performance degradation between Service B and Service C.
D. None of the above.

Answer: B
Explanation:

QUESTION NO: 14

The owner of a service inventory reports that the public key related to a certain private key has been lost. There is a concern that this was the result of a security breach. A security specialist recommends contacting the certificate authority in order to add the corresponding certificate to the certificate authority's Certificate Revocation List (CRL). However, the certificate authority responds

by indicating that this is not necessary. Which of the following answers explains this response?

A. The certificate authority needs to issue a new public key instead.
B. The certificate authority requires that the existing public key needs to be changed within the existing certificate.
C. Public keys cannot get lost because they are alreadypublicallyavailable.
D. None of the above

Answer: C
Explanation:

QUESTION NO: 15

A service contract includes a security policy that exposes specific details of the service's underlying implementation. This is an example of the application of which service-orientation principle?

A. Service Abstraction
B. Service Loose Coupling
C. Standardized Service Contract
D. None of the above.

Answer: D
Explanation:

QUESTION NO: 16

Which of the following security mechanisms can provide centralized security measures for all services within a service inventory?

A. public key infrastructure
B. single sign-on
C. hashed certificate repository
D. identity management system

Answer: A,B,D
Explanation: