QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

SOA

S90.18A

Fundamental SOA Security

QUESTION: 85
One of the primary industry standards used for the application of the Data Confidentiality pattern is:

A. XML-Encryption
B. Canonical XML
C. XML-Signature
D. SAML

Answer: A

QUESTION: 86
Which of the following design options can help reduce the amount of runtime processing required by security logic within a service composition?

A. Increase the usage of XML-Encryption and XML-Signature.
B. Use a single sign-on mechanism.
C. Introduce an identity store that is shared by the services within the service composition.
D. Ensure that non-repudiation is constantly guaranteed.

Answer: B

QUESTION: 87
A project team is planning to create a secure service composition that consists of services from two different domain service inventories. The security mechanisms for each service inventory are based on different vendor technologies that adhere to the same industry standards and the same design standards. What is wrong with this service composition architecture?

A. Because different vendor security technologies were used, services from different domain service inventories will be using incompatible security credentials.
B. Security mechanisms have a fixed limitation that prevents their usage across service inventory boundaries.
C. Vendor technologies do not adhere to industry standards. Only industry technologies adhere to industry standards.
D. None of the above

Answer: D

QUESTION: 88
Online Certificate Status Protocol (OCSP) based services provide online certificate revocation checking. However, these types of services can introduce network latency because only one certificate can be checked at a time.

A. True
B. False

Answer: A

QUESTION: 89
Atypical SAML assertion will contain at least one of the following subject statements:

A. authorization decision statement
B. authentication statement
C. attribute statement
D. certificate authority issuer statement

Answer: A, B, C

QUESTION: 90
Service A hashes a message using algorithm X. which creates message digest X1. Service B uses a different algorithm Y to create message digest Y1 of the same message. Which of the following statements are true regarding the comparison of X1 and Y1?

A. They have fixed sizes
B. They can be swapped
C. They do not match
D. They are based on the same hashing algorithm

Answer: A, C

QUESTION: 91
Security specialists at an organization require that messages exchanged between two services are kept private. There is an added requirement to check if the messages were

tampered with. The application of which of the following patterns fulfills these requirements?

A. Data Confidentiality
B. Data Origin Authentication
C. Direct Authentication
D. Brokered Authentication

Answer: A, B

QUESTION: 92
Username and X.509 token profiles can be combined so that a single message can contain a username token that is digitally signed.

A. True
B. False

Answer: A

QUESTION: 93
Service A is owned by Organization A. Service A sends a message containing confidential data to Service B, which is owned by Organization B. Service B sends the message to Service C, which is also owned by Organization B. Organization A trusts Organization B, which means there is no requirement to protect messages from intermediaries and after a message is received by Service B (and as long as the message remains within the boundary of Organization B), there is no requirement to keep the message data confidential. Which of the following approaches will fulfill these security requirements with the least amount of performance degradation?

A. Messages exchanged between Service A and Service B are encrypted using XML-Encryption.
B. The communication channel between Service A and Service B is encrypted using a transport- layer security technology.
C. SAML security tokens are used so that Service B can authenticate Service A.
D. An authentication broker is introduced between Service A and Service B.

Answer: B

QUESTION: 94

You are required to design security mechanisms to enable secure message exchanges between different domain service inventories within the same organization. This needs to be documented in the design specification for which type of service-oriented architecture?

A. service architecture
B. service composition architecture
C. service inventory architecture
D. service-oriented enterprise architecture

Answer: D

QUESTION: 95
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: 96
Which of the following tasks directly relates to the application of the Service Loose Coupling principle?

A. Creating one security policy that is shared by multiple services.
B. Creating one security policy that is specific to one service.
C. Creating multiple security policies that are specific to one service.
D. All of the above.

Answer: D

QUESTION: 97

Service A hashes a message, resulting in message digest X. Service A encrypts the message digest X with its private key, resulting ir ciphertext X1. Service A sends the message and X1 to Service B. Service B hashes the message, resulting in message digest Y. Service B decrypts X1 with Service A's public key, recovering message digest X. Service B compares Y with X and finds them to be equal. This proves that:

A. the message was not altered
B. only Service A sent this particular message
C. public key cryptography was used
D. Allof the above

Answer: D

QUESTION: 98
A typical SAML assertion will contain at least one of the following subject statements:

A. authorization decision statement
B. authentication statement
C. attribute statement
D. certificate authority issuer statement

Answer: A, B, C