Free Questions for S90.18 by dumpshq

Shared by Jennings on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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:

Options:

A- the message was not altered

B- only Service A sent this particular message

C- public key cryptography was used

D- All of the above

Answer:

D

Question 2

Question Type: MultipleChoice

Which of the following tasks directly relates to the application of the Service Loose Coupling principle?

Options:

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 3

Question Type: MultipleChoice

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

Options:

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 4

Question Type: **MultipleChoice**

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?

Options:

A- service architecture

B- service composition architecture

C- service inventory architecture

D- service-oriented enterprise architecture

Answer:

D

Question 5

Question Type: MultipleChoice

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?

Options:

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 6

Question Type: **MultipleChoice**

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

Options:

A- True

B- False

Answer:

A

Question 7

Question Type: MultipleChoice

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?

Options:

A- Data Confidentiality

B- Data Origin Authentication

C- Direct Authentication

D- Brokered Authentication

Answer:

A, B

Question 8

Question Type: MultipleChoice

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

Options:

A- authorization decision statement

B- authentication statement

C- attribute statement

D- certificate authority issuer statement

Answer:

A, B, C

Question 9

Question Type: MultipleChoice

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

Options:

A- XML-Encryption

B- Canonical XML

C- XML-Signature

D- SAML

Answer:

A

Question 10

Question Type: **MultipleChoice**

The communication between Service A and Service B needs to be kept private. A security specialist is planning to implement secret key cryptography in order to encrypt the messages. Which of the following approaches addresses this requirement?

Options:

A- Create a shared key that will be used by both the services for message encryption and decryption.

B- Both the services need to be built with support for the XML-Signature industry standard.

C- The Data Origin Authentication pattern needs to be applied across both service architectures.

D- None of the above.

Answer:

A