



Free Questions for S90.18 by go4braindumps

Shared by Berg on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

- 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 2

Question Type: MultipleChoice

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.

Options:

A- True

B- False

Answer:

A

Question 3

Question Type: MultipleChoice

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?

Options:

- 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 4

Question Type: MultipleChoice

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

Options:

- 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 5

Question Type: MultipleChoice

Which of the following industry standards enable non-repudiation?

Options:

- A- XML-Encryption
- B- XML-Signature
- C- SAML

D- None of the above

Answer:

B, C

Question 6

Question Type: MultipleChoice

The Data Origin Authentication pattern is applied to services throughout a service inventory. As a result, if malicious service intermediaries change data within messages exchanged by these services, such changes will be detected.

Options:

A- True

B- False

Answer:

A

Question 7

Question Type: MultipleChoice

To provide message confidentiality and message integrity, which of the following patterns need to be applied?

Options:

- A- Data Confidentiality and Direct Authentication
- B- Data Origin Authentication and Brokered Authentication
- C- Direct Authentication and Brokered Authentication
- D- None of the above

Answer:

D

Question 8

Question Type: MultipleChoice

A SAML assertion always contains:

Options:

- A- the name of the issuer
- B- a validity period
- C- subject confirmation
- D- signature

Answer:

A, B

Question 9

Question Type: MultipleChoice

A set of SAML tokens has been used as a result of the application of the Brokered Authentication pattern within a particular service inventory. Because SAML assertions normally contain a signature, the security specialist is confident that the integrity of messages will be maintained. What's wrong with this assumption?

Options:

- A- The signature contained within the SAML assertion protects the integrity of the assertion, not of the message itself.
- B- SAML assertions also contain the name of the issuer and the validity period, which are needed in addition to the signature to ensure message integrity.
- C- SAML assertions cannot contain signatures.
- D- Nothing is wrong. The security specialist's assumption is correct.

Answer:

A

Question 10

Question Type: MultipleChoice

The Brokered Authentication pattern needs to be used in conjunction with the Data Confidentiality and Data Origin Authentication patterns in order to ensure that claims held in security tokens remain secure and that the security tokens are actually issued by a valid authentication broker. What is wrong with this statement?

Options:

- A-** The Brokered Authentication pattern, the Data Origin Authentication pattern and the Data Confidentiality pattern cannot be used together.
- B-** Only the Brokered Authentication pattern and the Data Confidentiality pattern need to be applied together in order to ensure that claims held in security tokens remain secure.
- C-** The statement is correct if the Brokered Authentication pattern is substituted for the Direct Authentication pattern.
- D-** There is nothing wrong with this statement.

Answer:

D

To Get Premium Files for S90.18 Visit

<https://www.p2pexams.com/products/s90.18>

For More Free Questions Visit

<https://www.p2pexams.com/arcitura-education/pdf/s90.18>

