



**Free Questions for S90.18 by certsinside**

**Shared by Velazquez on 15-04-2024**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

## Question 1

---

**Question Type:** MultipleChoice

---

Security mechanisms that are based on vendor-specific security technology will always decrease the autonomy of services that are required to use these security mechanisms.

**Options:**

---

A- True

B- False

**Answer:**

---

B

## Question 2

---

**Question Type:** MultipleChoice

---

Service A supports WS-Security and Service B does not. How can they exchange secure messages?

**Options:**

---

- A-** WS-Security regulates identity stores and therefore does not prohibit Service A and Service B from exchanging secure messages.
- B-** Service B can be designed to support XML Canonicalization instead. This enables Service B to be compatible with any service that supports WS-Security.
- C-** As long as both services share the same public key. it doesn't matter whether WS-Security is supported.
- D-** None of the above.

**Answer:**

---

D

## Question 3

---

**Question Type: MultipleChoice**

---

Losing a \_\_\_\_\_ does not compromise the identity of the key owner, whereas losing a \_\_\_\_\_ does compromise the identity of the key owner.

**Options:**

---

- A- private key, public key
- B- validated certificate, revoked certificate
- C- security policy, SAML token
- D- None of the above

**Answer:**

---

D

## Question 4

---

**Question Type: MultipleChoice**

---

Which of the following are valid security considerations specific to the application of the Service Autonomy principle?

**Options:**

---

- A- Avoid including non-essential security requirements in the service contract.
- B- Avoid including content in the service contract that unnecessarily exposes details about the underlying service implementation.

- C-** Avoid modifying security policies that can break dependencies with service consumers.
- D-** None of the above.

**Answer:**

---

D

## Question 5

---

**Question Type:** MultipleChoice

---

The messages exchanged between two services are kept confidential by using symmetric encryption. The security specialist is quite strict about making sure that no attacker is able to intercept and decipher messages sent between these two services. As a result, periodic audits are conducted in order to ensure that shared keys are always kept confidential. A single shared key has been in use for quite some time now. The security specialist was confident that all keys were well guarded, but just recently their security was compromised. How is this possible given that the shared key was never lost?

**Options:**

---

- A-** Symmetric encryption is not intended for long-term use. It needs to be replaced with asymmetric encryption after some time.
- B-** The attackers somehow figured out which encryption algorithm was used. As a result, they were able to decipher the messages.

**C-** Because the same shared key was used for a long time, attackers were able to obtain the key by comparing messages sent between the two services.

**D-** The shared key was decoded by the attackers using algorithms from related private keys used during prior message exchanges.

**Answer:**

---

C

## Question 6

---

**Question Type:** MultipleChoice

---

Service A contains a service capability that runs a complex mathematical function, which results in runtime failure if invalid input values are supplied by a service consumer. Security needs to be added so that it can be verified that message content received by Service A has not been altered since the message was sent by a legitimate service consumer. Which pattern needs to be applied to fulfill this security requirement?

**Options:**

---

**A-** Data Confidentiality

**B-** Data Origin Authentication

C- Direct Authentication

D- Brokered Authentication

**Answer:**

---

B

**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>**

