Free Questions for S90.20 by vceexamstest

Shared by Daugherty on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

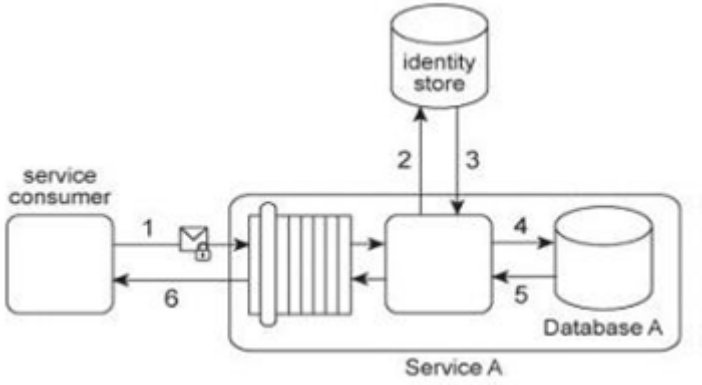
Question 1

Question Type: MultipleChoice

Service A provides a data access capability that can be used by a variety of service consumers. The database records accessed by Service A are classified as either private or public. There are two types of service consumers that use Service A:

Service consumers with public access permissions (allowed to access only public data records) and service consumers with private access permissions (allowed to access all data records). For performance reasons the Service A architecture uses a single database, named Database A .Each record in Database A is classified as either private or public. After Service A is invoked by a service consumer (1), it authenticates the request message using an identity store and retrieves the corresponding authorization (2, 3). Once authorized, the service consumer's request is submitted to Database A (4), which then returns the requested data (5) If the service consumer has private access permissions, all of the returned data is included in Service A's response message (6). If the service consumer has public access permissions, then Service A first filters the data in order to remove all unauthorized private data records, before sending to the response message to the service consumer (6). An investigation recently detected that private data has been leaked to unauthorized service consumers. An audit of the Service A architecture revealed that Service A's filtering logic is flawed, resulting in situations where private data was accidentally shared with service consumers that only have public access permissions. Further, it was discovered that attackers have been monitoring response messages sent by Service A in order to capture private data. It is subsequently decided to split Database A into two databases:

one containing only private data (the Private Database) and the other containing only public data (the Public Database). What additional changes are necessary to address these security problems?



Options:

A- The Service A logic needs to be modified to work with the two new databases. Service A needs to be able to access the Public Database and the Private Database when it receives a request message from a service consumer with private access permissions, and it must only access the Public Database when it receives a request message from a service consumer with public access permissions. Furthermore, any response messages issued by Service A containing private data need to be encrypted.

B- A utility service needs to be created and positioned between Service A and the service consumer. The utility service can-contain screening logic that can verify the service consumer's credentials and then forward the request message to the Private Database or to the Public Database, depending on the service consumer's access permissions. Because each request message is evaluated by the database, no filtering of the returned data is necessary. The data is sent back to the consumer in a response message encrypted using symmetric key encryption.

C- After the service consumer's request message is authenticated. Service A can generate a onetime symmetric encryption key that it sends to the service consumer. This key is encrypted by the public key of the service consumer. After the service consumer acknowledges the receipt of the one-time encryption key, Service A forwards the service consumer's data access request (and the corresponding credentials) to both databases. After receiving the responses from the databases, Service A compiles the results into a

single response message. This message is encrypted with the one-time key and sent by Service A to the service consumer.

D- The Service A architecture can be enhanced with certificate-based authentication of service consumers in order to avoid dependency on the identity store. By using digital certificates, Service A can authenticate a service consumer's request message and then forward the data access request to the appropriate database. After receiving the responses from the databases, Service A can use the service consumer's public key to encrypt the response message that is sent to the service consumer.

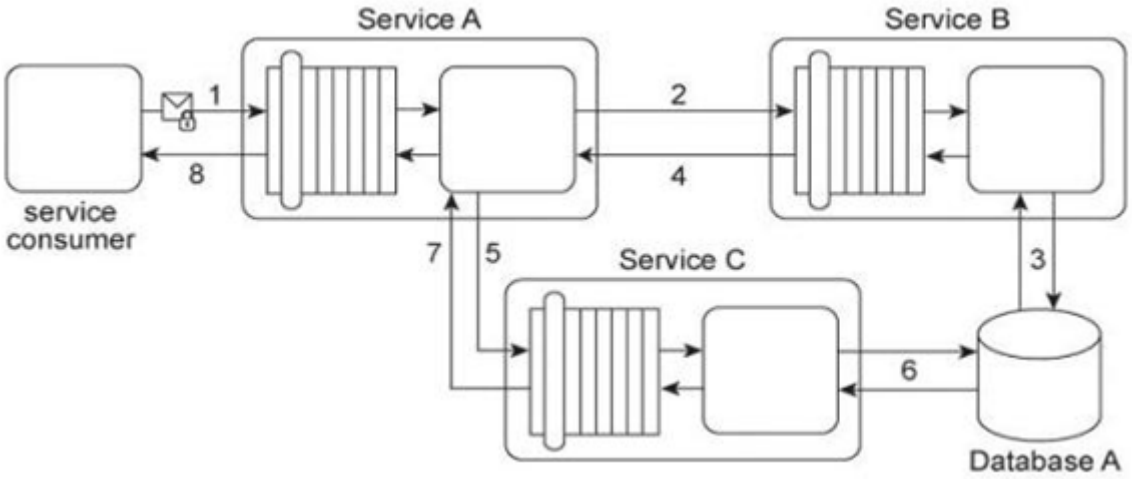
Answer:

A

Question 2

Question Type: **MultipleChoice**

Service A provides a customized report generating capability. Due to infrastructure limitations, the number of service consumers permitted to access Service A concurrently is strictly controlled. Service A validates request messages based on the supplied credentials (1). If the authentication of the request message is successful, Service A sends a message to Service B (2) to retrieve the required data from Database A (3). Service A stores the response from Service B (4) in memory and then issues a request message to Service C (5). Service C retrieves a different set of data from Database A (6) and sends the result back to Service A (7). Service A consolidates the data received from Services B and C and sends the generated report in the response message to the service consumer (8). It has been discovered that attackers have been gaining access to confidential data exchanged between Service A and Service B, and between Service A and its service consumers. What changes can be made to this service composition architecture in order to counter this threat?



Options:

A- Apply the Service Perimeter Guard pattern in order to protect message exchanges between Service A and its service-consumers. Apply the Direct Authentication pattern in order to protect message exchanges between Service A and Service B .

B- Apply the Direct Authentication pattern in order to protect message exchanges between Service A and its service consumers and between Service A and Service B .This approach will establish a password-based authentication mechanism that relies on a local identity store and will therefore prevent access by attackers.

C- Apply the Data Origin Authentication pattern to protect the final report sent by Service A to its service consumer. Service A can generate a message digest of the final report, after which it can sign the digest with its own private key. It then can send both the final report and the signed-message digest to its service consumer. This service consumer can generate its own message digest, decrypt the signed digest using the public key of Service A (which proves that Service A sent the message), and then compare the two digests. If the digests match, it guarantees that the final report was not tampered with during transmission.

D- None of the above

Answer:

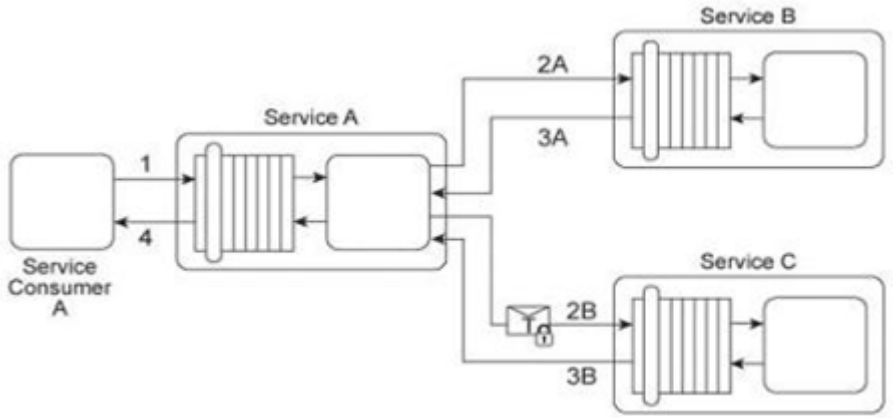
D

Question 3

Question Type: MultipleChoice

Service A is a publically accessible service that provides free multimedia retrieval capabilities to a range of service consumers. To carry out this functionality, Service A is first invoked by Service Consumer A (1). Based on the nature of the request message received from Service Consumer A, Service A either invokes Service B or Service C .When Service B is invoked by Service A (2A) it retrieves data from publicly available sources (not shown) and responds with the requested data (3A). When Service C is invoked by Service A (2B) it retrieves data from proprietary sources within the IT enterprise (not shown) and responds with the requested data (3B). After receiving a response from Service B or Service C, Service A sends the retrieved data to Service Consumer A (4). Service B does not require service consumers to be authenticated, but Service C does require authentication of service consumers. The service contract for Service A therefore uses WS-Policy alternative policies in order to express the two different authentication requirements to Service Consumer A .When Service Consumer A sends a request message (1), Service A determines whether the request requires the involvement of Service C and then checks to ensure that the necessary security credentials were received as part of the message. If the credentials provided by Service Consumer A are verified. Service A creates a signed SAML assertion and sends it with the request message to Service C (2B) This authentication information is protected by public key encryption However, responses to Service Consumer A's request message (3B, 4) are not encrypted for performance reasons. Recently, the usage of Service C has noticeably declined. An

investigation has revealed response messages issued by Service C (3B) have been repeatedly intercepted and accessed by unauthorized and malicious intermediaries. As a result, Service Consumer A has lost confidence in the use of Service A for the retrieval of proprietary data because it is being viewed as a security risk. This is especially troubling, because the owner of Service A had planned to start charging a fee for Service A's ability to provide proprietary data via the use of Service C .How can this service composition architecture be changed to address the security problem with minimal impact on runtime performance?



Options:

A- Use the existing PKI to provide message-layer security for the response messages originating from Service C .To provide-message confidentiality, Service C can encrypt the response messages using Service Consumer A's public key. This prevents unauthorized intermediaries from accessing the content of response messages.

B- Use the existing PKI to provide two-way authentication of the exchanged messages. After receiving a request from the service consumer, Service A can respond with a signed acknowledgement of the message, encrypted by the public key of Service Consumer A .Only Service Consumer A will be able to decrypt the encrypted acknowledgement. Service Consumer A then responds to the acknowledgement, thereby verifying its identity with Service A .Because both Service Consumer A and Service A are mutually

authenticated, end-to-end transport-layer security is sufficient to provide message confidentiality in order to prevent unauthorized intermediaries from accessing messages originating from Service C .

C- Use the existing PKI to establish secure communication between Service Consumer A and Service C .A symmetric key can be generated for the data being sent from Service C to Service Consumer A Service C can generate a session key that is encrypted with Service Consumer A's public key. Service C can then attach the session key to the response message, which is encrypted using the session key. Because only Service Consumer A can decrypt the encrypted session key, the data transmitted in the message is safe from access by unauthorized intermediaries.

D- Use the existing PKI to specify encryption and digital signature requirements on the messages. Service C can use Service-Consumer A's public key to generate a symmetric key. Service Consumer A can also generate the same session key from its own public key. Service C can use the session key to encrypt the response message (and the hash value of the response message), concatenate them, and send them to Service Consumer A .Service Consumer A separates the concatenated and encrypted hash value, decrypts it, and then decrypts the encrypted response message. As a result, the confidentiality and integrity of the response message are guaranteed.

Answer:

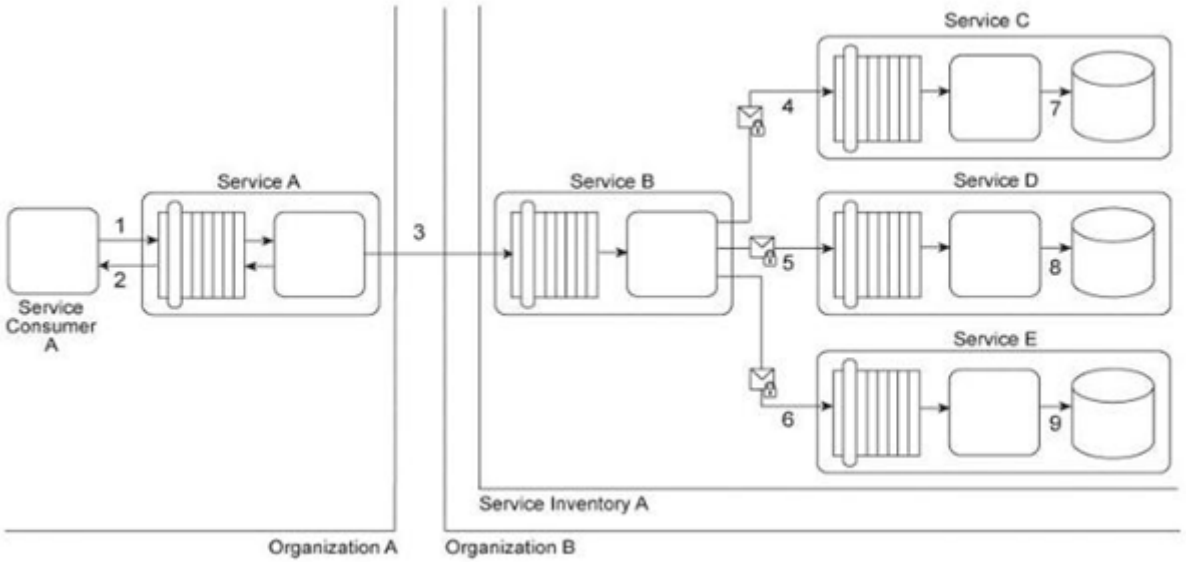
C

Question 4

Question Type: MultipleChoice

Service Consumer A sends a request to Service A (1). Service A replies with an acknowledgement message (2) and then processes the request and sends a request message to Service B (3). This message contains confidential financial data. Service B sends three

different request messages together with its security credentials to Services C, D, and E (4, 5, 6). Upon successful authentication, Services C, D, and E store the data from the message in separate databases (7, 8, 9) Services B, C, D, and E belong to Service Inventory A, which further belongs to Organization B .Service Consumer A and Service A belong to Organization A .The service contracts of Services A and B both comply with the same XML schema. However, each organization employs different security technologies for their service architectures. To protect the confidential financial data sent by Service A to Service B, each organization decides to independently apply the Data Confidentiality and the Data Origin Authentication patterns to establish message-layer security for external message exchanges. However, when an encrypted and digitally signed test message is sent by Service A to Service B, Service B was unable to decrypt the message. Which of the following statements describes a solution that solves this problem?



Options:

A- Although both of the organizations applied the Data Confidentiality and the Data Origin Authentication patterns, the security-technologies used for the Service A and Service B architectures may be incompatible. Because there are several technologies and versions of technologies that can be used to apply these patterns, the organizations need to standardize implementation level details of the relevant security technologies.

B- The problem with the test message occurred because Service A used incorrect keys to protect the message sent to Service B .Service A used its own public key to sign the message and then used Service B's public key to encrypt the message content. To correct the problem, Service A must use WS-Secure-Conversation to agree on a secret session key to be used to encrypt messages exchanged between Services A and B .Because this session key is only known by Services A and B, encrypting the messages with this key also provides authentication of the origin of the data.

C- Although both of the organizations successfully applied the Data Confidentiality and the Data Origin Authentication patterns, the order in which the patterns were applied is incorrect. The application of the Data Origin Authentication pattern must always follow the application of the Data Confidentiality pattern to ensure that the message confidentiality from a third party authenticates the origin of the message.

D- The problem with the test message occurred because Service A needed the private key of Service B to digitally sign the-message. An attacker pretending to be Service B likely sent a fake private/public keys pair to Service A .Using these fake keys to encrypt and digitally sign the message made the message incompatible for Service B .Because the fake private key was also used to sign the hash, it explains the source of the problem.

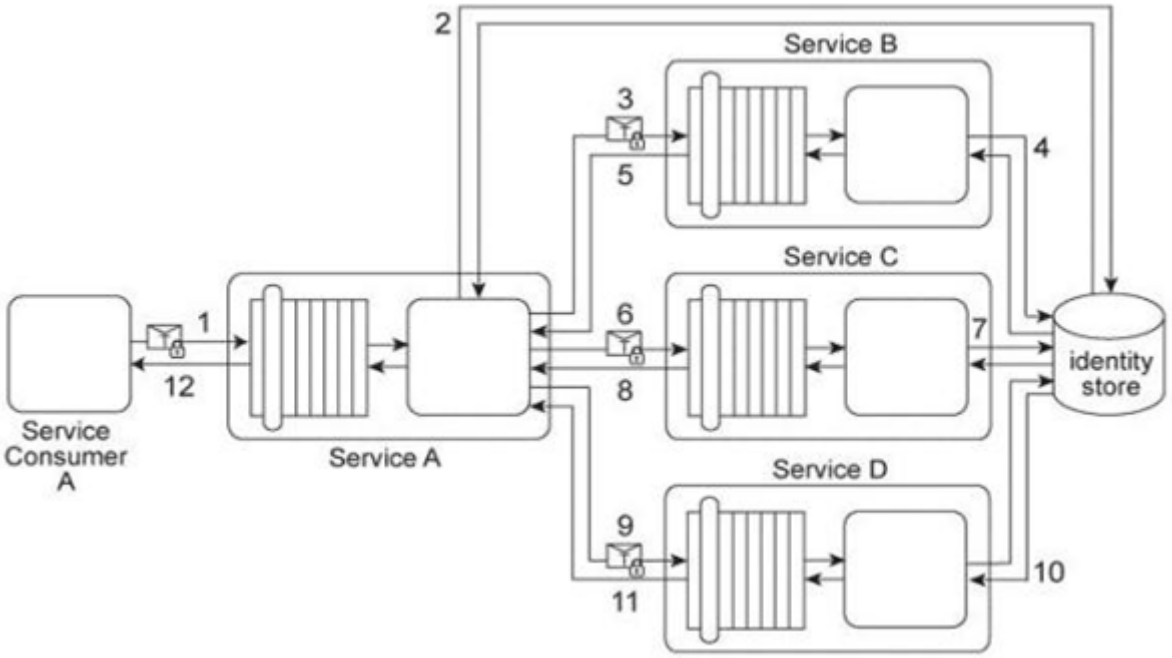
Answer:

A

Question 5

Question Type: **MultipleChoice**

Service Consumer A sends a request message with a Username token to Service A (1). Service B authenticates the request by verifying the security credentials from the Username token with a shared identity store (2), To process Service Consumer A's request message. Service A must use Services B, C, and D .Each of these three services also requires the Username token (3. 6, 9) in order to authenticate Service Consumer A by using the same shared identity store (4, 7, 10). Upon each successful authentication, each of the three services (B, C, and D) issues a response message back to Service A (5, 8, 11). Upon receiving and processing the data in all three response messages, Service A sends its own response message to Service Consumer A (12). There are plans implement a single sign-on security mechanism in this service composition architecture. The service contracts for Services A, C, and D can be modified with minimal impact in order to provide support for the additional messaging requirements of the single sign-on mechanism. However, Service B's service contract is tightly coupled to its implementation and, as a result, this type of change to its service contract is not possible as it would require too many modifications to the underlying service implementation. Given the fact that Service B's service contract cannot be changed to support single sign-on, how can a single sign-on mechanism still be implemented across all services?



Options:

A- Apply the Brokered Authentication pattern so that Service A acts as an authentication broker that issues a SAML token on behalf of Service Consumer A, and forwards this token to Services C and D .Create a new utility service is positioned between Service A and Service B .This utility service perform a conversion of the SAML token to a Username token, and then forwards the Username token to Service B so that Service B can still perform authentication of incoming requests using its own security mechanism.

B- Apply the Brokered Authentication pattern to establish Service A as an authentication broker that issues a SAML token for Service Consumer A and forwards Service Consumer A's token to other services. Apply the Trusted Subsystem pattern to create a utility service that acts as a trusted subsystem for Service B .This utility service is able to perform authentication using the SAML token from Service A

and can then generate a Username token by embedding its own credentials when accessing Service B .This way, Service B can perform authentication of requestmessages as it does now, but it can still participate in the single sign-on message exchanges without requiring changes to its service contract.

C- Apply the Brokered Authentication pattern so that Service A acts as an authentication broker that issues a SAML token for Service Consumer A and forwards Service Consumer A's token to Services C and D .Create a second service contract for Service B that supports single sign-on. This way, Service B can still perform authentication of incoming requests using the old service contract while allowing for the processing of SAML tokens using the new service contract.

D- Replace the Username tokens with X.509 digital certificates. This allows for the single sign-on mechanism to be implemented without requiring changes to any of the service contracts.

Answer:

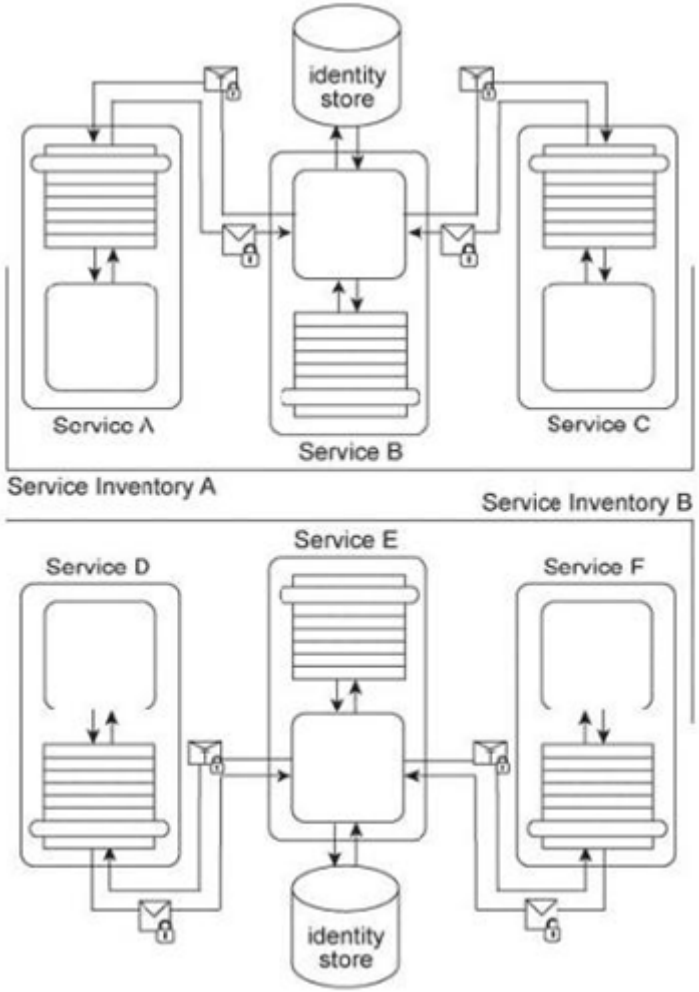
A

Question 6

Question Type: **MultipleChoice**

Services A, B, and C reside in Service Inventory A and Services D, E, and F reside in Service Inventory B .Service B is an authentication broker that issues WS-Trust based SAML tokens to Services A and C upon receiving security credentials from Services A and C .Service E is an authentication broker that issues WS-Trust based SAML tokens to Services D and F upon receiving security credentials from Services D and E .Service B uses the Service Inventory A identify store to validate the security credentials of Services A and C .Service E uses the Service Inventory B identity store to validate the security credentials of Services D and F .To date, the two service

inventories have existed independently from each other. However, a requirement has emerged that the services in Service Inventory A need to be able to use the services in Service Inventory B, and vice versa. How can cross-service inventory message exchanges be enabled with minimal changes to the existing service inventory architectures and without introducing new security mechanisms?



Options:

A- Because SAML tokens cannot be used across multiple security domains, authentication brokers C and E need to be replaced with one single authentication broker so that one token issuer is used for all services across both of the service inventories.

B- The current security mechanism already fulfills the requirement because SAML tokens can be used across multiple security-domains. The only change required is for each authentication broker to be configured so that it issues service inventory-specific assertions for SAML tokens originating from other service inventories.

C- The individual domain service inventories need to be combined into one enterprise service inventory. The Service Perimeter Guard pattern can be applied to establish a contact point for request messages originating from outside the service inventory. Within the service inventory, services no longer need to be authenticated because they are all part of the same trust boundary.

D- The Trusted Subsystem pattern is applied to encapsulate Services B and E using a central utility service that balances request and response messages exchanged between Services B and E, depending on which service inventory the messages originate from. The utility service also contains transformation logic to ensure that the SAML tokens issued by Services B and E are compatible. This guarantees that an issued SAML token can be used across Service Inventories A and B without further need for runtime conversion.

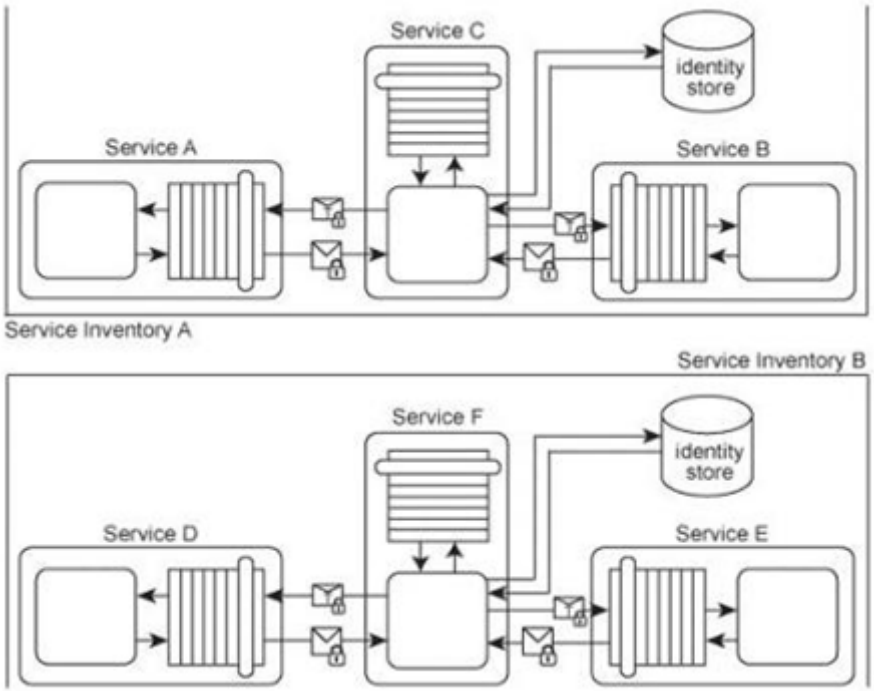
Answer:

B

Question 7

Question Type: MultipleChoice

Services A, B and C belong to Service Inventory A .Services D, E and F belong to Service Inventory B .Service C acts as an authentication broker for Service Inventory A .Service F acts as an authentication broker for Service Inventory B .Both of the authentication brokers use Kerberos-based authentication technologies. Upon receiving a request message from a service consumer, Services C and F authenticate the request using a local identity store and then use a separate Ticket Granting Service (not shown) to issue the Kerberos ticket to the service consumer. A recent security audit of the two service inventories revealed that both authentication brokers have been victims of attacks. In Service Inventory A, the attacker has been intercepting and modifying the credential information sent by Service C (the ticket requester) to the Ticket Granting Service. As a result, the requests have been invalidated and incorrectly rejected by the Ticket Granting Service. In Service Inventory B, the attacker has been obtaining service consumer credentials and has used them to request and receive valid tickets from the Ticket Granting Service. The attacker has then used these tickets to enable malicious service consumers to gain access to other services within the service inventory. How can the two service inventory security architectures be improved in order to counter these attacks?



Options:

A- The Data Confidentiality pattern can be applied to messages exchanged by the services in Service Inventory A .The Data Origin Authentication pattern can be applied to messages exchanged by services in Service Inventory B .

B- The Service Perimeter Guard pattern can be applied to Service Inventory A in order to establish a perimeter service responsible for validating and filtering all incoming request messages on behalf of Service C .The Data Origin Authentication pattern can be applied to messages exchanged by services in Service Inventory B .This will ensure the integrity of messages by verifying their origins to the message recipients.

C- WS-Secure-Conversation can be used to secure the communication between the authentication broker and service consumers in Service Inventory A .This ensures that Services A and B will contact Service C to request a security context token that will be used to generates a session key for the encryption of the ticket submitted to Service C . The Data Origin Authentication pattern can be applied to messages exchanged by services in Service Inventory B .This will ensure the integrity of messages try verifying their origins to the message recipients.

D- WS-Trust can be used to establish secure communication between the authentication broker and the service consumers. After receiving the request message and the corresponding credentials from service consumers, the authentication broker can validate their identity, and if successful, a signed SAML assertion containing all authentication information will be issued. The SAML assertion will then be used to authenticate the service consumers during subsequent communications. Because the messages are signed and encrypted, malicious service consumers cannot access the data. This approach can be applied to counter the threats in both Service Inventories A and B .

Answer:

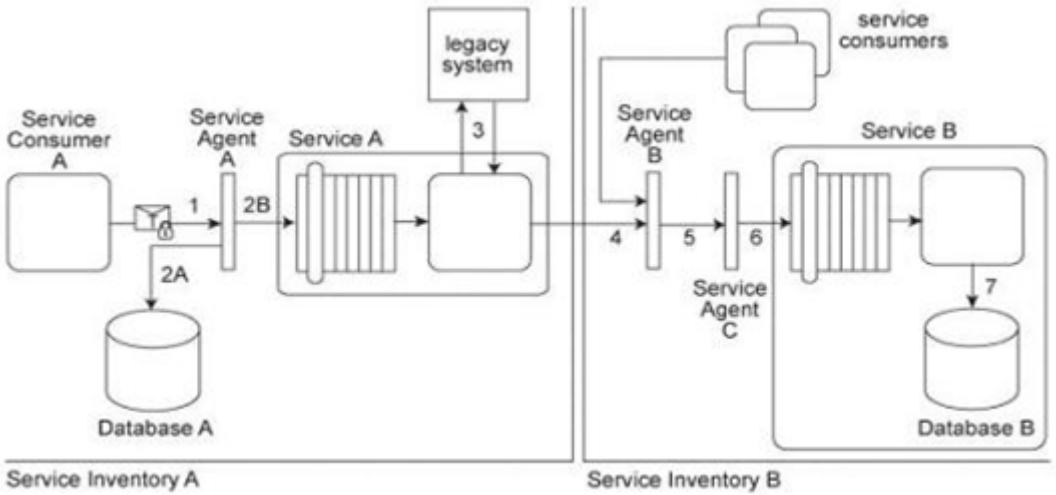
A

Question 8

Question Type: **MultipleChoice**

Service Consumer A sends a request message with an authentication token to Service A, but before the message reaches Service A, it is intercepted by Service Agent A (1). Service Agent A validates the security credentials and also validates whether the message is compliant with Security Policy A .If either validation fails, Service Agent A rejects the request message and writes an error log to

Database A (2A). If both validations succeed, the request message is sent to Service A (2B). Service A retrieves additional data from a legacy system (3) and then submits a request message to Service B Before arriving at Service B, the request message is intercepted by Service Agent B (4) which validates its compliance with Security Policy SIB then Service Agent C (5) which validates its compliance with Security Policy B .If either of these validations fails, an error message is sent back to Service A .that then forwards it to Service Agent A so that it the error can be logged in Database A (2A). If both validations succeed, the request message is sent to Service B (6). Service B subsequently stores the data from the message in Database B (7). Service A and Service Agent A reside in Service Inventory A .Service B and Service Agents B and C reside in Service Inventory B .Security Policy SIB is used by all services that reside in Service Inventory B .Service B can also be invoked by other service consumers from Service Inventory B .Request messages sent by these service consumers must also be compliant with Security Policies SIB and B .Access to the legacy system in Service Inventory A is currently only possible via Service A, which means messages must be validated for compliance with Security Policy A .A new requirement has emerged to allow services from Service Inventory B to access the legacy system via a new perimeter service that will be dedicated to processing request messages from services residing in Service Inventory B .Because the legacy system has no security features, all security processing will need to be carried out by the perimeter service. However, there are parts of Security Policy A that are specific to Service A and do not apply to the legacy system or the perimeter service. Furthermore, response messages sent by the perimeter service to services from Service Inventory B will still need to be validated for compliance to Security Policy B and Security Policy SIB .How can the Policy Centralization pattern be correctly applied without compromising the policy compliance requirements of services in both service inventories?



Options:

A- In order for Security Policy A to be centralized so that it can be shared by Service A and the new perimeter service, messages sent to the perimeter service from services in Service Inventory B will need to continue complying with Security Policy A, even if it requires that the messages contain content that does not relate to accessing the legacy system. In order to centralize Security-Policy B it will need to be combined with Security Policy SIB, which means that the functionality within Service Agents B and C can be combined into a single service agent.

B- A single centralized security policy can be created by combining Security Policy A, Security Policy B .and Security Policy SIB into a single security policy that is shared by services in both Service Inventory A and Service Inventory B .This means that the new perimeter service can share the same new security policy with Service A .This further simplifies message exchange processing because request messages sent by services in Service Inventory B to the new perimeter service need to comply to the same security policy as the response messages sent back by the perimeter service to the services in Service Inventory B .

C- The parts of Security Policy A that are required for access to the new perimeter service need to be removed and placed into a new security policy that is shared by Service A and the perimeter service. Messages sent by services accessing the perimeter service from Service Inventory B will need to be compliant with the new security policy. Because the perimeter service is dedicated to message exchange with services from Service Inventory B, response messages sent by the perimeter service can be designed for compliance to Security Policy B and Security Policy SIB .

D- Due to the amount of overlap among Security Policy A, Security Policy B, and Security Policy SIB, the Policy Centralization pattern cannot be correctly applied to enable the described message exchange between the perimeter service in Service Inventory A and services in Service Inventory B .

Answer:

C