DUMPSQUEEN

SOA Security Lab

SOA S90.20

Version Demo

Total Demo Questions: 5

Total Premium Questions: 30

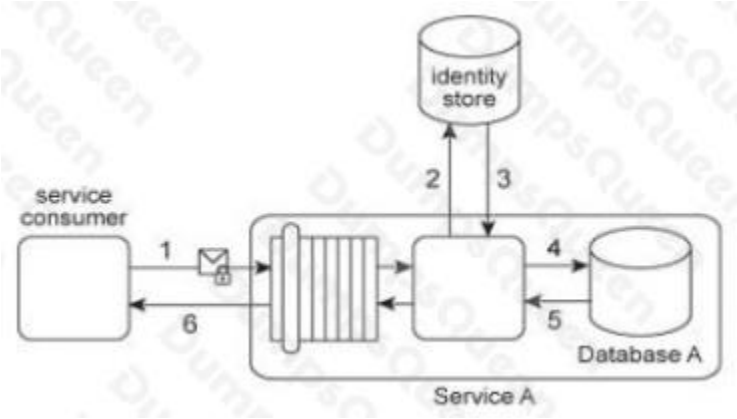
Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

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?

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 one-time 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.

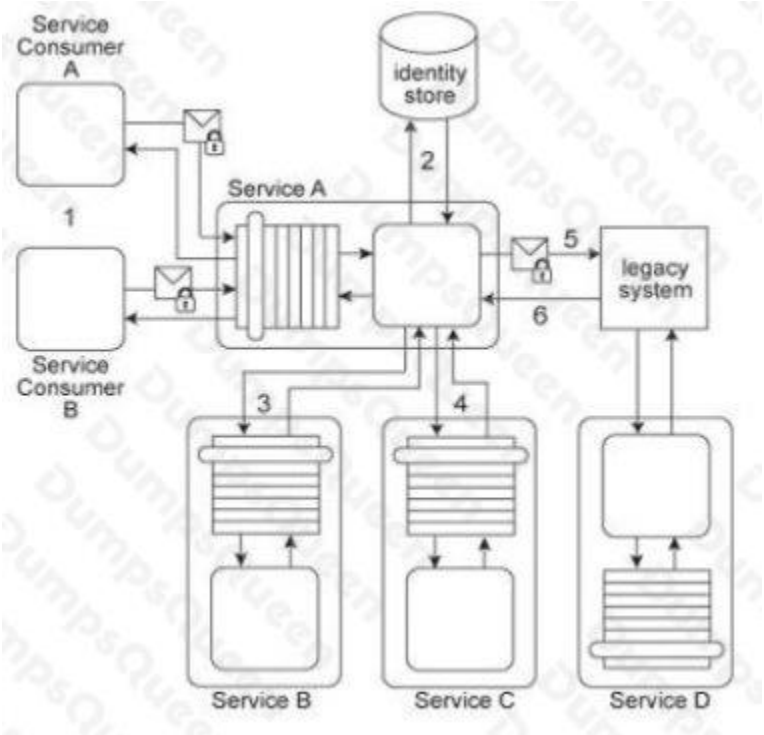
D. The Service A architecture can be enhanced with certificate-based authentication of service consumers in order to avoid dependency on the identity store. By using digital certificates, Service A can authenticate a service consumer's request message and then forward the data access request to the appropriate 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 NO: 2

Service A has two specific service consumers, Service Consumer A and Service Consumer B (1). Both service consumers are required to provide security credentials in order for Service A to perform authentication using an identity store (2). If a service consumer's request message is successfully authenticated, Service A processes the request by exchanging messages with Service B (3) and then Service C (4). With each of these message exchanges, Service A collects data necessary to perform a query against historical data stored in a proprietary legacy system. Service A's request to the legacy system must be authenticated (5). The legacy system only provides access control using a single account. If the request from Service A is permitted, it will be able to access all of the data stored in the legacy system. If the request is not permitted, none of the data stored in the legacy system can be accessed. Upon successfully retrieving the requested data (6), Service A generates a response message that is sent back to either Service Consumer A or B.

The legacy system is also used independently by Service D without requiring any authentication. Furthermore, the legacy system has no auditing feature and therefore cannot record when data access from Service A or Service D occurs. If the legacy system encounters an error when processing a request, it generates descriptive error codes.



This service composition architecture needs to be upgraded in order to fulfill the following new security requirements: 1. Service Consumers A and B have different permission levels, and therefore, response messages sent to a service consumer

must only contain data for which the service consumer is authorized. 2. All data access requests made to the legacy system must be logged. 3. Services B and C must be provided with the identity of Service A's service consumer in order to provide Service A with the requested data. 4. Response messages generated by Service A cannot contain confidential error information about the legacy system.

Which of the following statements provides solutions that satisfy these requirements?

A. To correctly enforce access privileges, Services B and C must share the identity store with Service A and directly authenticate Service Consumer A or B. Furthermore, Services B and C must each maintain two policies: one for Service Consumer A and one for Service Consumer B. After receiving a request message from a Service Services B and C must evaluate the validity of the request by using the identity store and the appropriate policy. Service Consumers A and B are required to submit the necessary security credentials to the legacy system as part of the request message sent to Service After verifying the credentials, the legacy system either performs the necessary processing or sends the response to Service A or denies access and sends an error message directly to Service Consumer A or B. The Message Screening pattern is applied to Service A so that it can perform message screening logic in order to filter out unauthorized data coming from the legacy system.

B. Apply the Trusted Subsystem pattern by introducing a new utility service that encapsulates data access to the legacy system. After Service A authenticates a service consumer it creates a signed SAML assertion containing authentication and authorization information. The SAML assertions are used by Service A to convey the identity information of Service Consumer A or B to Services B and C. The utility service filters response messages to the service consumer based on the information in the SAML assertions. The utility service keeps a log of the all data access requests made to the legacy system. The Exception Shielding pattern is further applied to the utility service in order to prevent the leakage of confidential error information.

C. Apply the Service Perimeter Guard pattern to provide selective access privileges to Service Consumers A and B. The resulting perimeter service shares the identity store with Service A, which it uses to authenticate each request message. If authentication is successful, the request message is forwarded to Service A. Service A then also authenticates the service consumer and retrieves the service consumer's security profile from the identity store upon successful authentication. Each service consumer's security profile includes its authorized level of access. Service consumer authentication is subsequently performed using digital certificates. The Exception Shielding pattern is further applied to the perimeter service in order to prevent the leakage of confidential error information.

D. Apply the Trusted Subsystem pattern by introducing a new utility service that encapsulates data access to the legacy system. The utility service evaluates request messages by authenticating the service consumer against the identity store and also verifying the digital signature of each request. If the request is permitted, Service A forwards the service consumer's credentials to Services B and C, and to the legacy system. The response messages from Services B and C are returned to Service A, while responses from the legacy system are processed by the utility service. Logic is added to the utility service so that it can log access requests made to the legacy system.

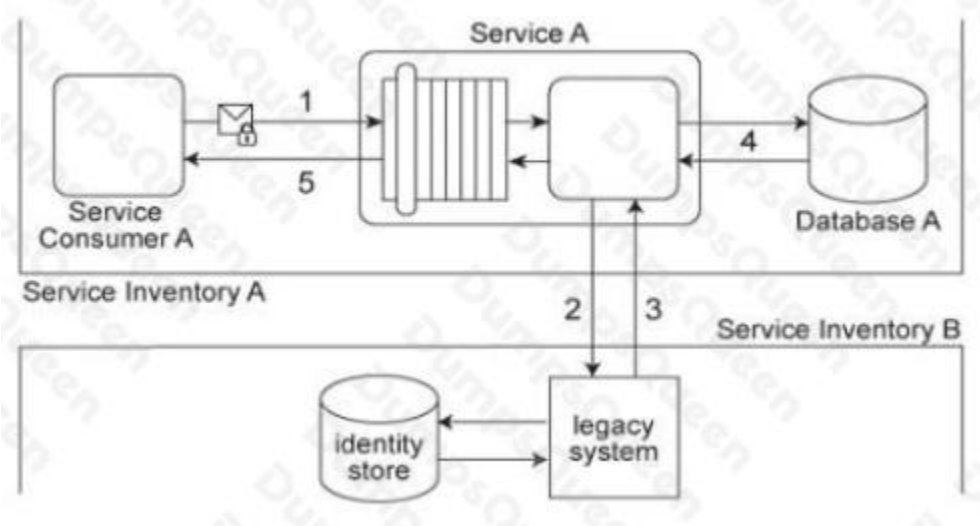
ANSWER: B

QUESTION NO: 3

Service Consumer A submits a request message with security credentials to Service A (1). The identity store that Service A needs to use in order to authenticate the security credentials can only be accessed via a legacy system that resides in a different service inventory. Therefore, to authenticate Service Consumer A, Service A must first forward the security credentials to the legacy system (2). The legacy system then returns the requested identity to Service A (3). Service A authenticates Service Consumer A against the identity received from the legacy system. If the authentication is successful, Service A retrieves the requested data from Database A (4), and returns the data in a response message sent back to Service Consumer A (5).

Service A belongs to Service Inventory A which further belongs to Security Domain A and the legacy system belongs to Service Inventory B which further belongs to Security Domain B. (The legacy system is encapsulated by other services

within Service Inventory B, which are not shown in the diagram.) These two security domains trust each other. Communication between Service A and the legacy system is kept confidential using transport-layer security.



No intermediary service agents currently exist between the two service inventories. However, it has been announced that due to the introduction of new systems, some intermediary service agents may be implemented in the near future. Additionally, the legacy system has been scheduled for retirement and will be replaced by a new identity management system that will provide a new identity store. Because the new identity store will need to serve many different systems, there are concerns that it could become a performance bottleneck. As a result, services (including Service A and other services in Security Domains A and B) will not be allowed to directly access the new identity store.

Which of the following statements describes a solution that can accommodate the requirements of the new identity store, the authentication requirements of Service A, and can further ensure that message exchanges between Security Domains A and B remain confidential after intermediary service agents are introduced?

A. Apply the Trusted Subsystem pattern to implement a utility service abstracting the new identity management system. Service A forwards Service Consumer As credentials to the utility service to verify Service Consumer As identity. The utility service authenticates the request originating from Service After successful authentication, the utility service uses its own credentials to retrieve the requested identity, and then send the identity to Service A, Therefore, effectively reducing the processing need of the identity management system. The current transport-layer security can still be used, in order to secure the communication between Service A and the new utility service, as it more efficient than the message-layer security.

B. Apply the Trusted Subsystem pattern by abstracting away the new identity management system using a utility service that authenticates the request from Service A and then uses its own credentials to retrieve the requested identity from the new identity management system. For the utility service to authenticate Service As request, it needs to be provisioned with a new identity database that contains identities for all authorized service consumers of the new utility service. In order to secure the communication between Service A and the new utility service, use message-layer security as it provides security over multiple hops considering the need to secure the message in case an intermediary is introduced in future.

C. Replicate the identity database used by the new identity management system. Because the Security Domains A and B trust each other, protection of the identity store is guaranteed. Use Service Agents to monitor changes to the identity database used by the new identity management system and to update the replica. This would satisfy the security needs of Service A, would eliminate the need to request services from Service Inventory B, and ensure that current identity information is available for Service A. Because Service A would not need to access services across different trust domains, the current transport-layer security is sufficient.

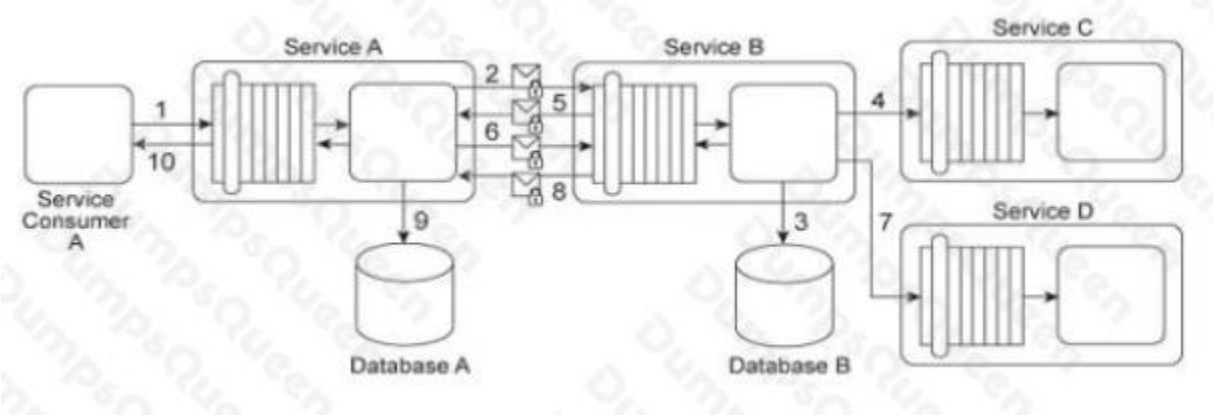
D. Apply the Brokered Authentication pattern to establish an authentication broker. Instead of Service A directly authenticating Service Consumer A, Service Consumer A submits a request message with security credentials to the authentication broker, which authenticates Service Consumer A against the new identity store and then issues a SAML token

to Service Consumer A that it can use for message exchanges with other services, if necessary. In order to secure cross-service inventory message exchanges, the Data Confidentiality pattern is applied to establish message-layer security.

ANSWER: D

QUESTION NO: 4

Service Consumer A sends a request message to Service A (1), after which Service A sends a request message with security credentials to Service B (2). Service B authenticates the request and, if the authentication is successful, writes data from the request message into Database B (3). Service B then sends a request message to Service C (4), which is not required to issue a response message. Service B then sends a response message back to Service A (5). After processing Service B's response, Service A sends another request message with security credentials to Service B (6). After successfully authenticating this second request message from Service A, Service B sends a request message to Service D (7). Service D is also not required to issue a response message. Finally, Service B sends a response message to Service A (8), after which Service A records the response message contents in Database A (9) before sending its own response message to Service Consumer A (10).



Services A and B use digital certificates to support message integrity and authentication. With every message exchange between the two services (2, 5, 6, 8), the digital certificates are used. It has been determined that both Databases A and B are vulnerable to malicious attackers that may try to directly access sensitive data records. Furthermore, performance logs have revealed that the current exchange of digital certificates between Services A and B is unacceptably slow.

How can the integrity and authenticity of messages exchanged between Services A and B be maintained, but with improved runtime performance - and - how can Databases A and B be protected with minimal additional impact on performance?

A. Apply the Brokered Authentication pattern to establish an authentication broker that uses WS-Trust based SAML tokens for message exchanges between Services A and B. This eliminates the need for Service A to be repeatedly authenticated by Service B. Use the public key of Service A to encrypt Database A and use the public key of Service B to encrypt Database B.

B. Apply the Brokered Authentication pattern to establish an authentication broker that uses WS-SecureConversation security context tokens (SCTs) to generate and transmit a symmetric session key. The session key is used to encrypt and digitally sign messages exchanged between Services A and For each database the Trusted Subsystem pattern is applied to require authenticated access to the database and to prevent attackers from accessing the database directly

C. Apply the Direct Authentication pattern to establish mutual authentication between Services A and B using a shared identity store. Service A attaches a Username token to the first request message sent to Service B and Service B authenticates the request message using the shared identity store. Similarly, when Service B submits a response message to Service A. it attaches its own Username token that Service A then authenticates by also using the same shared identity

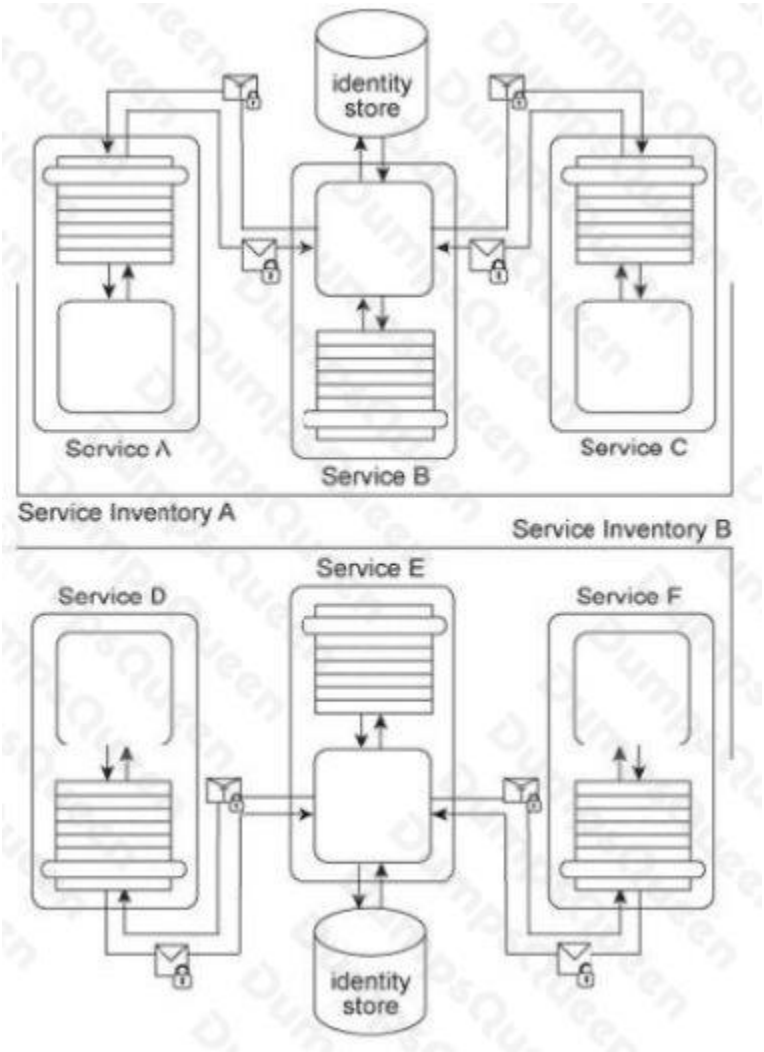
store. Database A is encrypted using the Service A password as a secret encryption key and Database B is encrypted using the Service B password as a secret encryption key.

D. Apply the Brokered Authentication pattern to establish an authentication broker that uses WS-Trust based SAML tokens for message exchanges between Services A and B. This eliminates the need for Service A to be repeatedly authenticated by Service B. Database A is encrypted using the Service A password as a secret encryption key and Database B is encrypted using the Service B password as a secret encryption key.

ANSWER: B

QUESTION NO: 5

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?

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