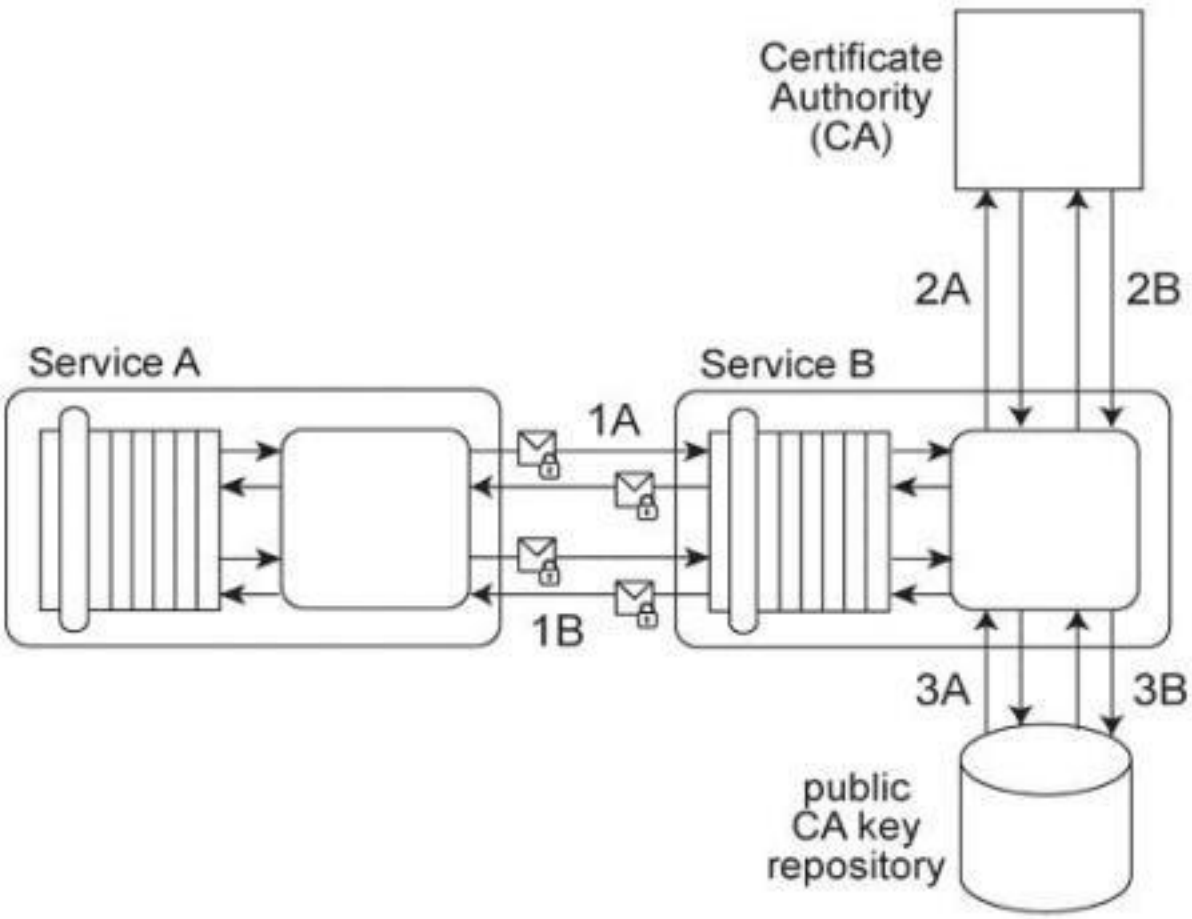
Exam : **S90.20**

Title : SOA Security Lab

Vendor : Arcitura

Version : DEMO

NO.1 Service A exchanges messages with Service B multiple times during the same runtime service activity. Communication between Services A and B has been secured using transport-layer security. With each service request message sent to Service B (1A. IB), Service A includes an X.509 certificate, signed by an external Certificate Authority (CA).
Service B validates the certificate by retrieving the public key of the CA (2A. 2B) and verifying the digital signature of the X.509 certificate. Service B then performs a certificate revocation check against a separate external CA repository (3A, 3B). No intermediary service agents reside between Service A and Service B.



To fulfill a new security requirement, Service A needs to be able to verify that the response message sent by Service B has not been modified during transit. Secondly, the runtime performance between Services A and B has been unacceptably poor and therefore must be improved without losing the ability to verify Service A's security credentials. It has been determined that the latency is being caused by redundant security processing carried out by Service B.
Which of the following statements describes a solution that fulfills these requirements?
A. The Data Origin Authentication pattern can be applied together with the Service Perimeter Guard pattern to establish a perimeter service that can verify incoming request messages sent to Service B and to filter response messages sent to Service A.
The repository containing the verification information about the Certificate Authorities can be replicated in the trust domain of the perimeter service. When access is requested by Service A, the perimeter service evaluates submitted security credentials by checking them against the locally replicated repository. Furthermore, it can encrypt messages sent to Service A by Service B.
and attach a signed hash value.

B. Service B needs to be redesigned so that it performs the verification of request messages from Service A only for the first message exchange during the runtime service activity. Thereafter, it can issue a SAML token to Service A that gets stored within the current session. Service A then uses this session-based token with subsequent message exchanges. Because SAML tokens have a very small validity period (in contrast to X.509 certificates), there is no need to perform a revocation check with every message exchange.

C. Apply the Trusted Subsystem pattern to introduce a utility service that performs the security processing instead of Service B.

The utility service can verify the security credentials of request messages from Service A and digitally sign messages sent to Service A to enable verification of message integrity. Furthermore, the utility service can perform the verification of security credentials submitted by Service A only once per runtime service activity. After the first message exchange, it can issue a SAML token to Service A that gets stored within the current session. Service A can then use this session- based token with subsequent message exchange. Because SAML tokens have a very small validity period (in contrast to X.509 certificates), there is no need to perform a revocation check with every message exchange.

D. WS-SecurityPolicy transport binding assertions can be used to improve performance via transport-layer security The use of symmetric keys can keep the encryption and decryption overhead to a minimum, which will further reduce the latency between Service A and Service B.

By encrypting the messages, attackers cannot modify message contents, so no additional actions for integrity verification are needed.

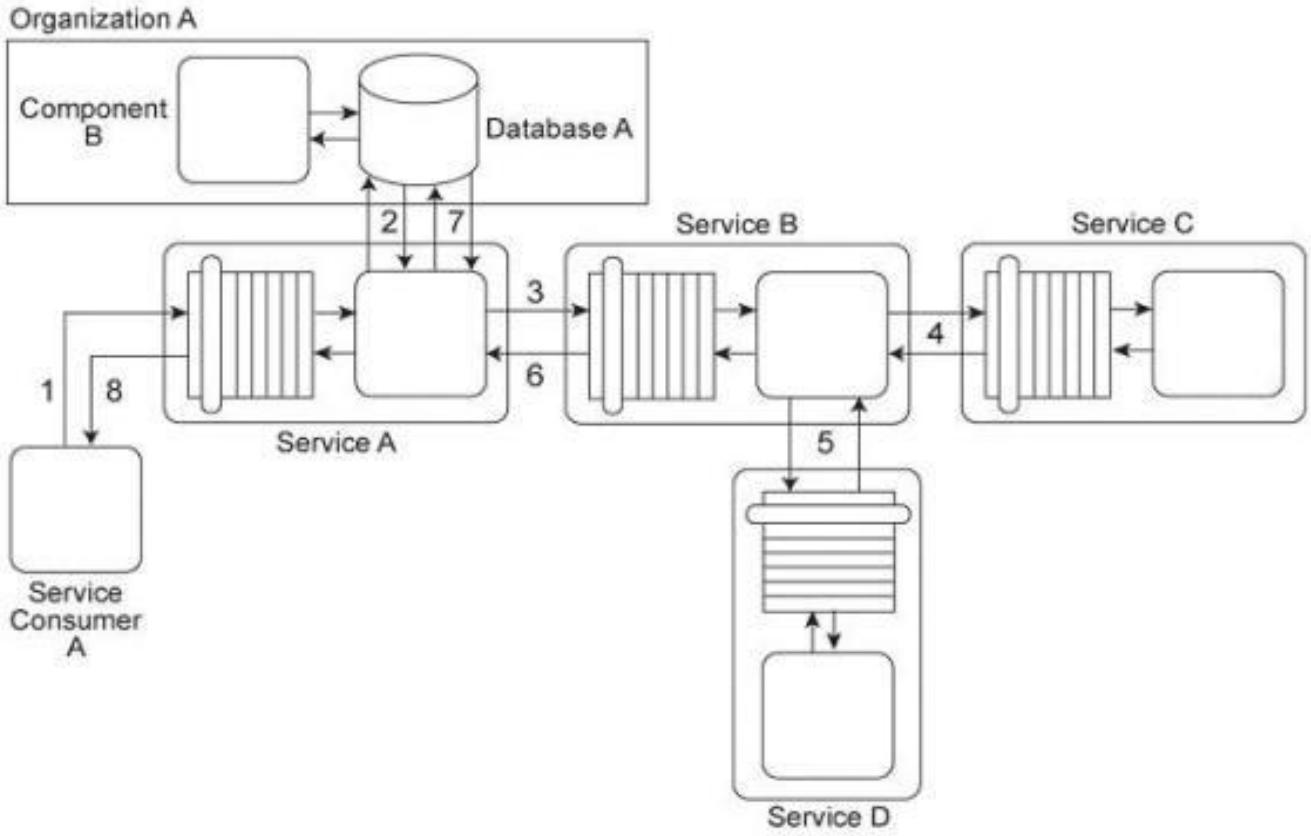
Answer: C

NO.2 Service Consumer A sends a request message to Service A (1) after which Service A retrieves financial data from Database A (2). Service A then sends a request message with the retrieved data to Service B (3). Service B exchanges messages with Service C (4) and Service D (5), which perform a series of calculations on the data and return the results to Service A.

Service A uses these results to update Database A (7) and finally sends a response message to Service Consumer A (8). Component B has direct, independent access to Database A and is fully trusted by Database A.

Both Component B and Database A reside within Organization A.

Service Consumer A and Services A, B, C, and D are external to the organizational boundary of Organization A.



Service A has recently experienced an increase in the number of requests from Service Consumer A. However, the owner of Service Consumer A has denied that Service Consumer A actually sent these requests. Upon further investigation it was determined that several of these disclaimed requests resulted in a strange behavior in Database A, including the retrieval of confidential data. The database product used for Database A has no feature that enables authentication of consumers. Furthermore, the external service composition (Services A, B, C, D) must continue to operate at a high level of runtime performance.

How can this architecture be improved to avoid unauthenticated access to Database A while minimizing the performance impact on the external service composition?

A. Implement a firewall between Service Consumer A and Service A.

All access to Service A is then controlled by the firewall rules. The firewall contains embedded logic that authenticates request messages and then forwards permitted messages to Service A. Moreover, the firewall can implement the Message Screening pattern so that each incoming message is screened for malicious content. This solution minimizes the security processing performed by Service A in order to maintain the performance requirements of the external service composition.

B. A utility service is established to encapsulate Database A and to carry out the authentication of all access to the database by Service A and any other service consumers.

To further support this functionality within the utility service, an identity store is introduced. This identity store is also used by Service A which is upgraded with its own authentication logic to avoid access by malicious service consumers pretending to be legitimate service consumers. In order to avoid redundant authentication by services within the external service composition, Service A creates a signed SAML assertion that contains the service consumer's authentication and authorization information.

C. The Brokered Authentication pattern is applied so that each service consumer generates a pair of private/public keys and sends the public key to Service A.

When any service in the external service composition (Services A, B, C, and D) sends a request message to another service, the request message is signed with the private key of the requesting service (the service acting as the service consumer). The service then authenticates the request using the already established public key of the service consumer. If authentication is successful, the service generates a symmetric session key and uses the public key of the service consumer to securely send the session key back to the service consumer. All further communication is protected by symmetric key encryption. Because all service consumers are authenticated, all external access to Database A is secured.

D. Service Consumer A generates a pair of private/public keys (Public Key E and Private Key D) and sends the public key to Service

Service A can use this key to send confidential messages to Service Consumer A because messages encrypted by the public key of Service Consumer A can only be decrypted by Service A The Data Origin Authentication pattern can be further applied so that Service A can authenticate Service Consumer A by verifying the digital signature on request messages. The Message Screening pattern is applied to a utility service that encapsulates Database A in order to prevent harmful input.

Answer: B

NO.3 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).

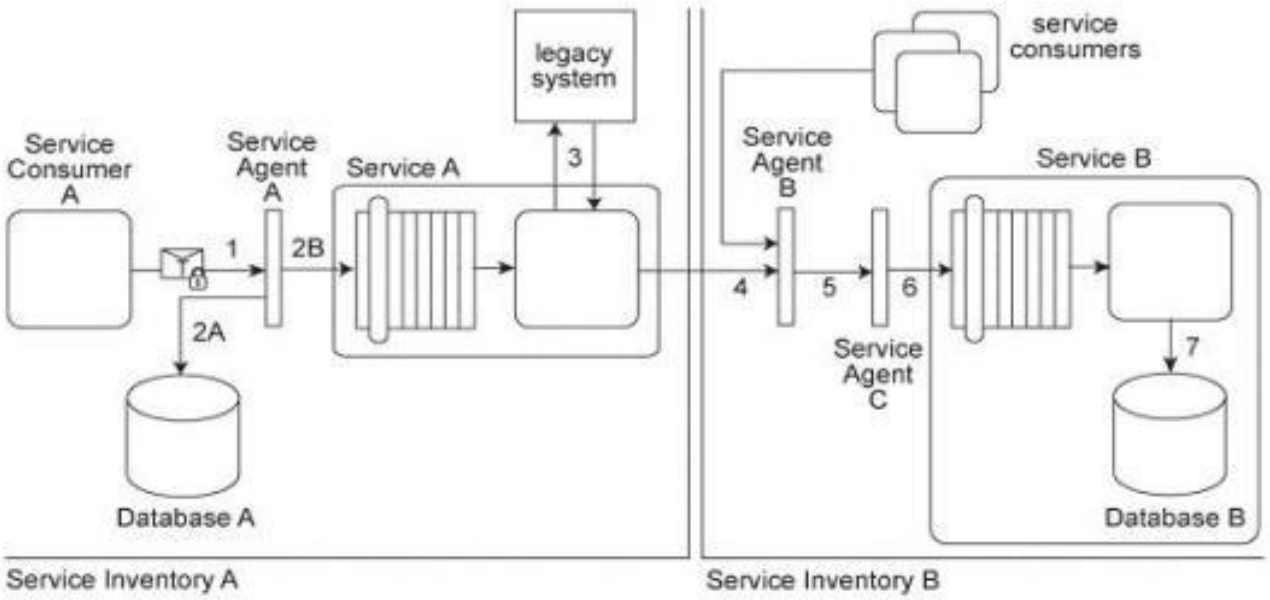
Service A and Service Agent A reside in Service Inventory A.

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 from within Service Inventory B.

Request messages sent by these service consumers must also be compliant with Security Policies SIB and B.



New services are being planned for Service Inventory A.
To accommodate service inventory-wide security requirements, a new security policy (Security Policy SIA) has been created. Compliance to Security Policy SIA will be required by all services within Service Inventory A.
Some parts of Security Policy A and Security Policy SIB are redundant with Security Policy SIA.
How can the Policy Centralization pattern be correctly applied to Service Inventory A without changing the message exchange requirements of the service composition?

A. The parts of Security Policy A and Security Policy SIB that are redundant with Security Policy SIA are removed so that there is no overlap among these three security policies.
Service Agent A is updated so that it can validate messages for compliance with both Security Policy A and Security Policy SIA. Service Agent B is updated so that it can validate messages for compliance with both Security Policy SIA and Security Policy SIB.
Service Agent C remains unchanged.

B. The parts of Security Policy A and Security Policy SIB that are redundant with Security Policy SIA are removed so that there is no overlap among these three security policies. A new service agent is introduced into Service Inventory A to validate compliance to the new Security Policy SIA prior to messages being validated by Service Agent
Another new service agent is introduced into Service Inventory B to validate compliance to the new Security Policy SIA prior to messages being validated by Service Agents B and C.

C. The parts of Security Policy A that are redundant with Security Policy SIA are removed so that there is no overlap between these two security policies. A new service agent is introduced into Service Inventory A to validate compliance to the new Security Policy SIA prior to messages being validated by Service Agent A.

D. Due to the amount of overlap among Security Policy A, Security Policy SIA, and Security Policy SIB, the Policy Centralization pattern cannot be correctly applied without changing the message exchange requirements of the service composition.

Answer: C