Vendor: SOA

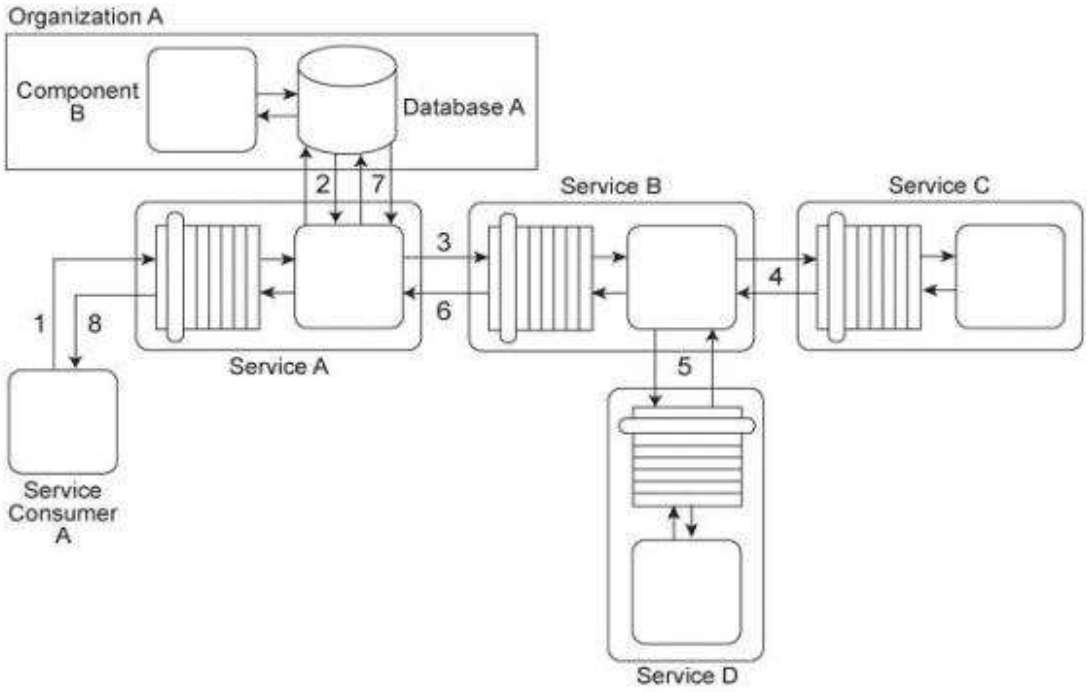
Exam Code: S90-20A

Exam Name: SOA Security Lab

Version: DEMO

QUESTION NO: 1

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.



Component B is considered a mission critical program that requires guaranteed access to and fast response from Database A. Service A was recently the victim of a denial of service attack, which resulted in Database A becoming unavailable for extended periods of time (which further compromised Component B). Additionally, Services B, C, and D have repeatedly been victims of malicious intermediary attacks, which have further destabilized the performance of Service A.

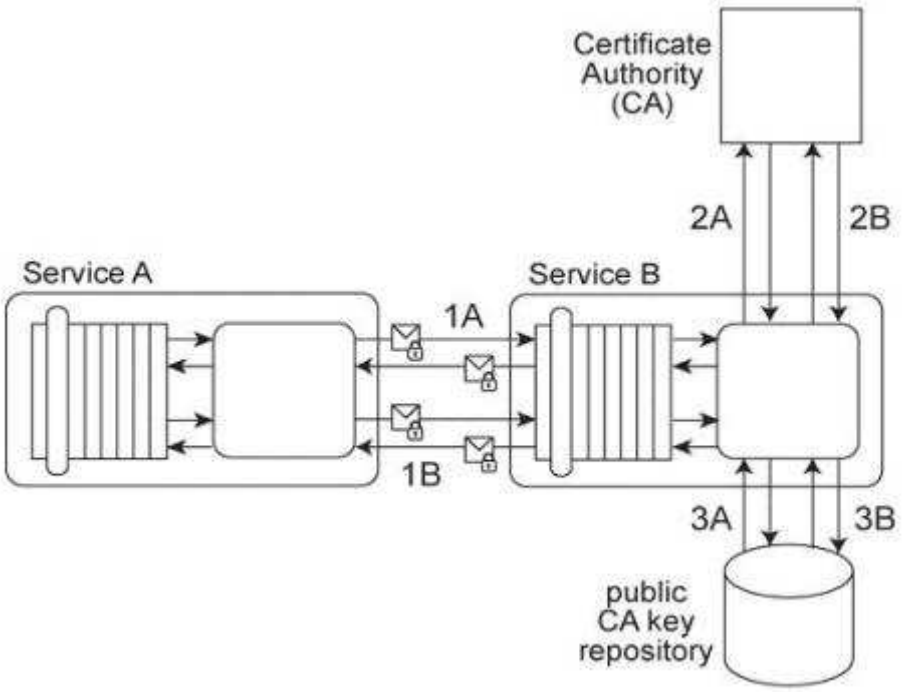
How can this architecture be improved to prevent these attacks?

A. A utility service is created to encapsulate Database A and to assume responsibility for authenticating all access to the database by Service A and any other service consumers. Due to the mission critical requirements of Component B, the utility service further contains logic that strictly limits the amount of concurrent requests made to Database A from outside the organizational boundary. The Data Confidentiality and Data Origin Authentication patterns are applied to all message exchanged within the external service composition in order to establish message-layer security.

B. Service Consumer A generates a private/public key pair and sends this public key and identity information to Service A. Service A generates its own private/public key pair and sends

it back to Service Consumer A. Service Consumer A uses the public key of Service A to encrypt a randomly generated session key and then sign the encrypted session key with the private key. The encrypted, signed session key is sent to Service A. Now, this session key can be used for secure message-layer communication between Service Consumer A and Service A. The Service Perimeter Guard pattern is applied to establish a perimeter service that encapsulates Database A in order to authenticate all external access requests.
C. Services B, C, and D randomly generate Session Key K, and use this key to encrypt request and response messages with symmetric encryption. Session Key K is further encrypted itself asymmetrically. When each service acts as a service consumer by invoking another service, it decrypts the encrypted Session Key K and the invoked service uses the key to decrypt the encrypted response. Database A is replicated so that only the replicated version of the database can be accessed by Service A and other external service consumers.
D. The Direct Authentication pattern is applied so that when Service Consumer A submits security credentials, Service A will be able to evaluate the credentials in order to authenticate the request message. If the request message is permitted, Service A invokes the other services and accesses Database A. Database A is replicated so that only the replicated version of the database can be accessed by Service A and other external service consumers.
Answer: A

QUESTION NO: 2
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. 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.

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. 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.

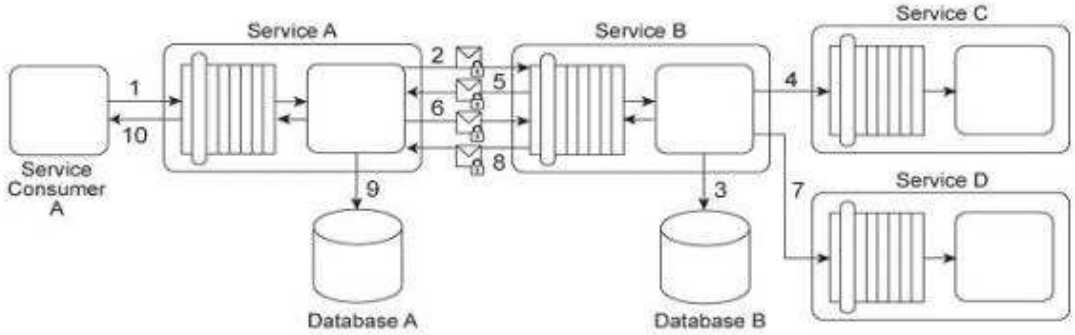
D. The Data Origin Authentication pattern can be applied together with the Service Perimeter Guard pattern to establish a perimeter service that can verify incoming request messages sent to Service B and to filter response messages sent to Service A. The repository containing the verification information 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.

Answer: A

QUESTION NO: 3

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 WSTrust 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 WSSecureConversation securitycontext 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 B. 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 identitystore. 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 WSTrust 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