QUESTIONS & ANSWERS

Kill your exam at first Attempt

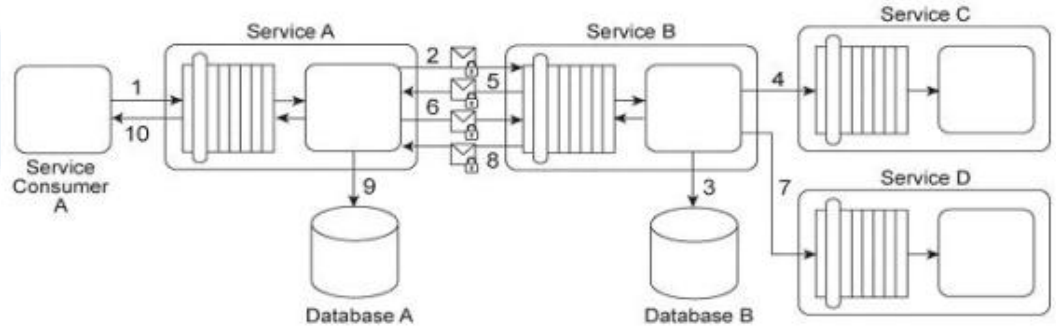
KILL EXAMS

SOA

S90.20A

SOA Security Lab

QUESTION: 27
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).

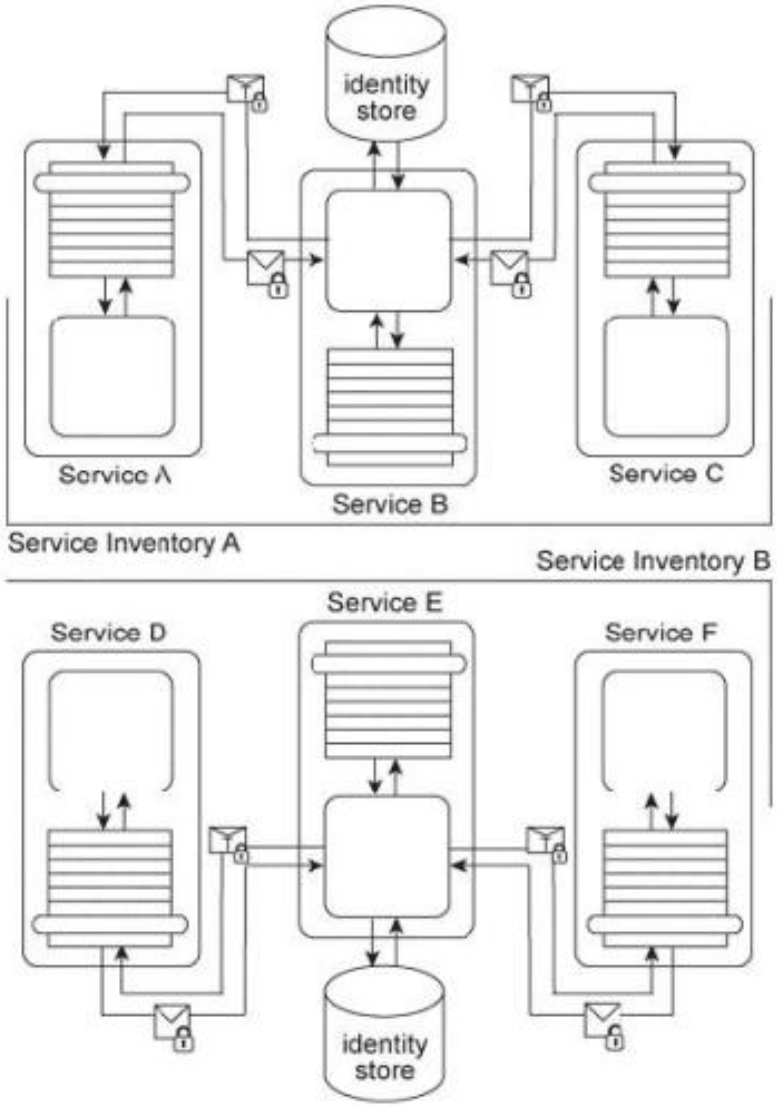


To use Service A, Service Consumer A is charged a per usage fee. The owner of Service Consumer A has filed a complaint with the owner of Service A, stating that the bills that have been issued are for more usage of Service A than Service Consumer A actually used. Additionally, it has been discovered that malicious intermediaries are intercepting and modifying messages being sent from Service B to Services C and D. Because Services C and D do not issue response messages, the resulting errors and problems were not reported back to Service B. Which of the following statements describes a solution that correctly addresses these problems? A. The Data Confidentiality and Data Origin Authentication patterns need to be applied in order to establish message-layerconfidentiality and integrity for messages sent to Services C and D. The Direct Authentication pattern can be applied to require that service consumer be authenticated in order to use Service A.
B. Messages sent to Services C and D must be protected using transport-layer encryption in order to ensure data confidentiality. Service consumers of Service A must be authenticated using X.509 certificates because they can be reused for several request messages.
C. Apply the Service Perimeter Guard and the Message Screening patterns together to establish a perimeter service between Service Consumer A and Service A. The perimeter service screens and authenticates incoming request messages from Service Consumer A. After successful authentication, the perimeter service generates a signed SAML assertion that is used by the subsequent services to authenticate and authorize the request message and is also carried forward as the security credential included in messages sent to Services C and D.
D. Apply the Brokered Authentication to establish an authentication broker between Service Consumer A and Service A that can carry out the Kerberos authentication

protocol. Before invoking Service A, Service Consumer A must request a ticket granting ticket and then it must request service granting tickets to all services in the service composition, including Services C and D. Messages sent by Service B to Services C and D must further be encrypted with the public key of Service Consumer A.

Answer: A

QUESTION: 28
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.



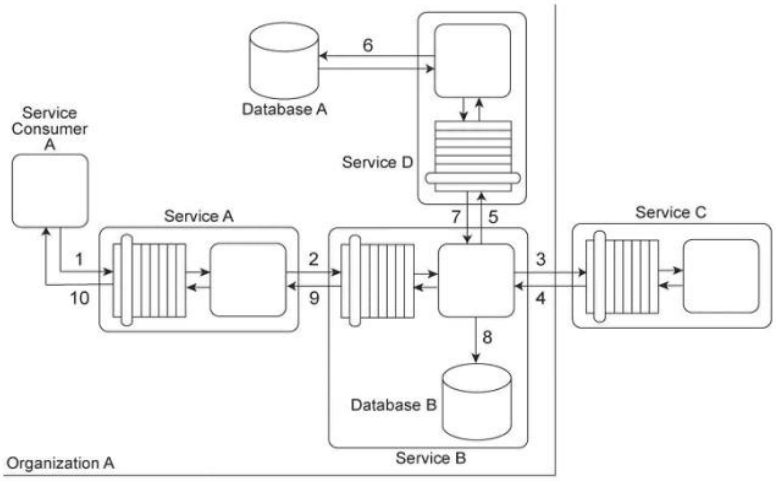
It is decided to use Service E as the sole authentication broker for all services in Service Inventories A and B. Service B is kept as a secondary authentication broker for load

balancing purposes. Specifically, it is to be used for situations where authentication requests are expected to be extra time consuming in order to limit the performance burden on Service E. Even though Service B has all the necessary functionality to fulfill this new responsibility, only Service E can issue SAML tokens to other services. How can these architectures be modified to support these new requirements?

A. When time consuming authentication requests are identified, Service E can forward them to Service B. Upon performing the authentication,Service B sends its own signed SAML token to Service E. Because Service E trusts Service B. it can use the Service B-specific SAML token to issue an official SAML token that is then sent to the original service consumer (that requested authentication) and further used by other services.
B. To provide load balancing, a service agent needs to be implemented to intercept all incoming requests to Service E. Theservice agent uses a random distribution of the authentication requests between Service B and Service E. Because the request messages are distributed in a random manner, the load between the two authentication brokers is balanced.
C. Because both Service B and Service E issue SAML tokens, these tokens are interchangeable. In order for both services toreceive the same amount of authentication requests, a shared key needs to be provided to them for signing the SAML tokens. By signing the SAML tokens with the same key, the SAML tokens generated by Service B cannot be distinguished from the SAML tokens generated by Service E.
D. Because the federation requirements ask for SAML tokens generated by Service E, Service B cannot function as anauthentication broker. To address the load balancing requirement, a new utility service needs to be introduced to provide functionality that is redundant with Service E. This essentially establishes a secondary authentication broker to which Service E can defer time- consuming authentication tasks at runtime.

Answer: B

QUESTION: 29
Service Consumer A sends a request message to Service A (1), after which Service A sends a request message to Service B (2). Service B forwards the message to have its contents calculated by Service C (3). After receiving the results of the calculations via a response message from Service C (4), Service B then requests additional data by sending a request message to Service D (5). Service D retrieves the necessary data from Database A (6), formats it into an XML document, and sends the response message containing the XML-formatted data to Service B (7). Service B appends this XML document with the calculation results received from Service C, and then records the entire contents of the XML document into Database B (8). Finally, Service B sends a response message to Service A (9) and Service A sends a response message to Service Consumer A (10).



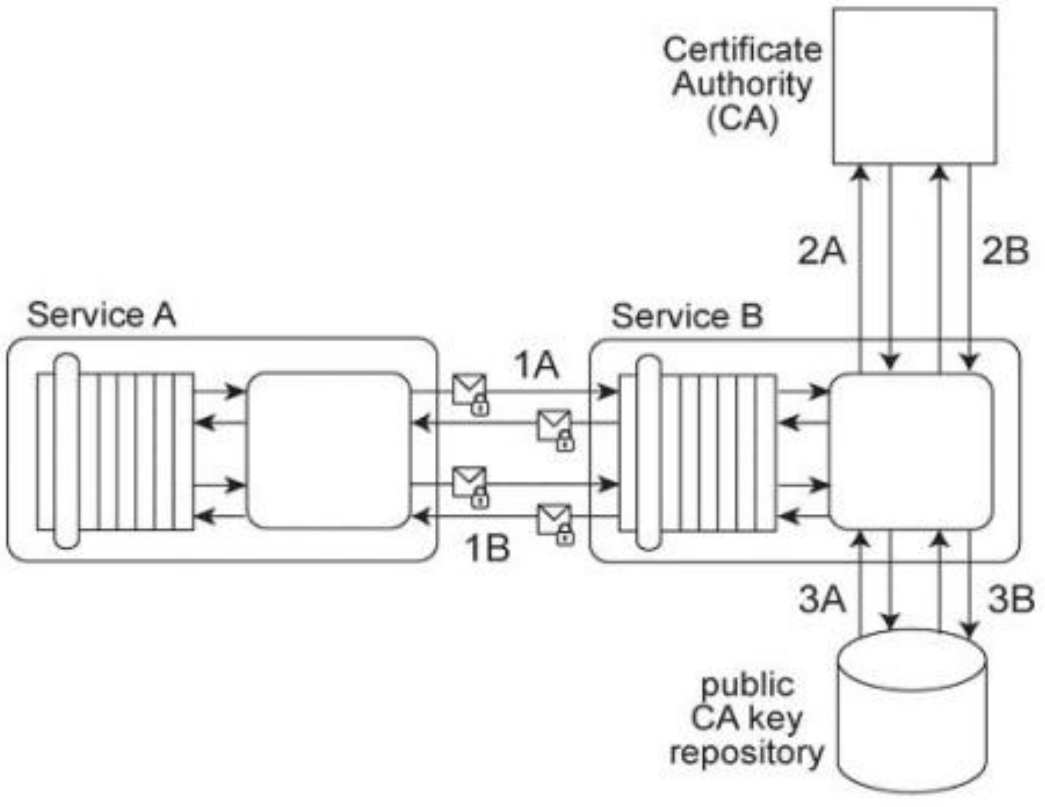
Services A, B and D are agnostic services that belong to Organization A and are also being reused in other service compositions. Service C is a publicly accessible calculation service that resides outside of the organizational boundary. Database A is a shared database used by other systems within Organization A and Database B is dedicated to exclusive access by Service B. Service B has recently been experiencing a large increase in the volume of incoming request messages. It has been determined that most of these request messages were auto-generated and not legitimate. As a result, there is a strong suspicion that the request messages originated from an attacker attempting to carry out denial-of-service attacks on Service B. Additionally, several of the response messages that have been sent to Service A from Service B contained URI references to external XML schemas that would need to be downloaded in order to parse the message data. It has been confirmed that these external URI references originated with data sent to Service B by Service C. The XML parser currently being used by Service A is configured to download any required XML schemas by default. This configuration cannot be changed. What steps can be taken to improve the service composition architecture in order to avoid future denial-of-service attacks against Service B and to further protect Service A from data access- oriented attacks?

A. Apply the Data Origin Authentication pattern so that Service B can verify that request messages that claim to have been sent by Service A actually did originate from Service A. Applythe Message Screening pattern to add logic to Service A so that it can verify that external URIs in response messages from Service B refer to trusted sources.
B. Apply the Service Perimeter Guard pattern to establish a perimeter service between Service B and Service C. Apply theBrokered Authentication pattern by turning the perimeter service into an authentication broker that is capable of ensuring that only legitimate response messages are being sent to Service C from Service B Further apply the Data Origin Authentication pattern to enable
the perimeter service to verify that messages that claim to have been sent by Service C actually originated from Service C. Apply the Message Screening pattern to add logic to the perimeter service to also verify that URIs in request messages are validated against a list of permitted URIs from where XML schema downloads have been pre-approved.
C. Apply the Service Perimeter Guard pattern and the Message Screening pattern together to establish a service perimeter guard that can filter response messages from Service C before they reach Services A and B. The filtering rules are based on the IP address of Service C. If a request message originates from an IP address not listed as one of the IP addresses associated with Service C. then the response message is rejected.

D. Apply the Direct Authentication pattern so that Service C is required to provide security credentials, such as Username tokens, with any response messages it sends to Service B. Furthermore, add logic to Service A so that it can validate security credentials passed to it via response messages from Service B. by using an identity store that is shared by Services A and B.

Answer: A

QUESTION: 30
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.



Service B has recently suffered from poor runtime performance plus it has been the victim of an access-oriented attack. As a result, its security architecture must be changed to fulfill the following new requirements: 1. The performance of security-related processing carried out by Service B when communicating with Service A must be improved. 2. All request messages sent from Service A to Service B must be screened to ensure that they do not contain malicious content. Which of the following statements describes a solution that fulfills these requirements?

A. Eliminate the need to retrieve the public key from the Certificate Authority and to verify the certificate revocation information by extending the service contract of Service B to accept certificates only from pre-registered Certificate Authorities. This form of pre-registration ensures that Service B has the public key of the corresponding Certificate Authority.
B. Add a service agent to screen messages sent from Service A to Service B. The service agent can reject any message containing malicious content so that only verified messages are passed through to Service B. Instead of using X.509 certificates, use WS-SecureConversation sessions. Service A can request a Security Context Token (SCT) from a Security Token Service and use the derived keys from the session key to secure communication with Service B. Service B retrieves the session key from the Security Token Service.
C. Apply the Trusted Subsystem pattern by introducing a new utility service between Service A and Service B. When Service A sends request messages, the utility service verifies the provided credentials and creates a customized security profile for Service A. The security profile contains authentication and access control statements that are then inherited by all subsequent request messages issued by Service A. As a result, performance is improved because Service A does not need to resubmit any additional credentials during subsequent message exchanged as part of the same runtime service activity. Furthermore, the utility service performs message screening logic to filter out malicious content.
D. Apply the Trusted Subsystem pattern to by introducing a new utility service. Because Service B is required to limit the use of external resources. Service A must ensure that no other services can request processing from Service B in order to prevent malicious content from infiltrating messages. This is achieved by creating a dedicated replica of Service B to be used by the utility service only. Upon receiving the request message and the accompanying security credentials from Service A. the utility service verifies the authentication information and the validity of the X.509 signature. If the authentication information is correct, then the utility service replicates the code of Service B, performs the necessary processing, and returns the response to Service A.

Answer: B