Arcitura Education

S90-20A Exam

Arcitura Education SOA Security Lab Exam

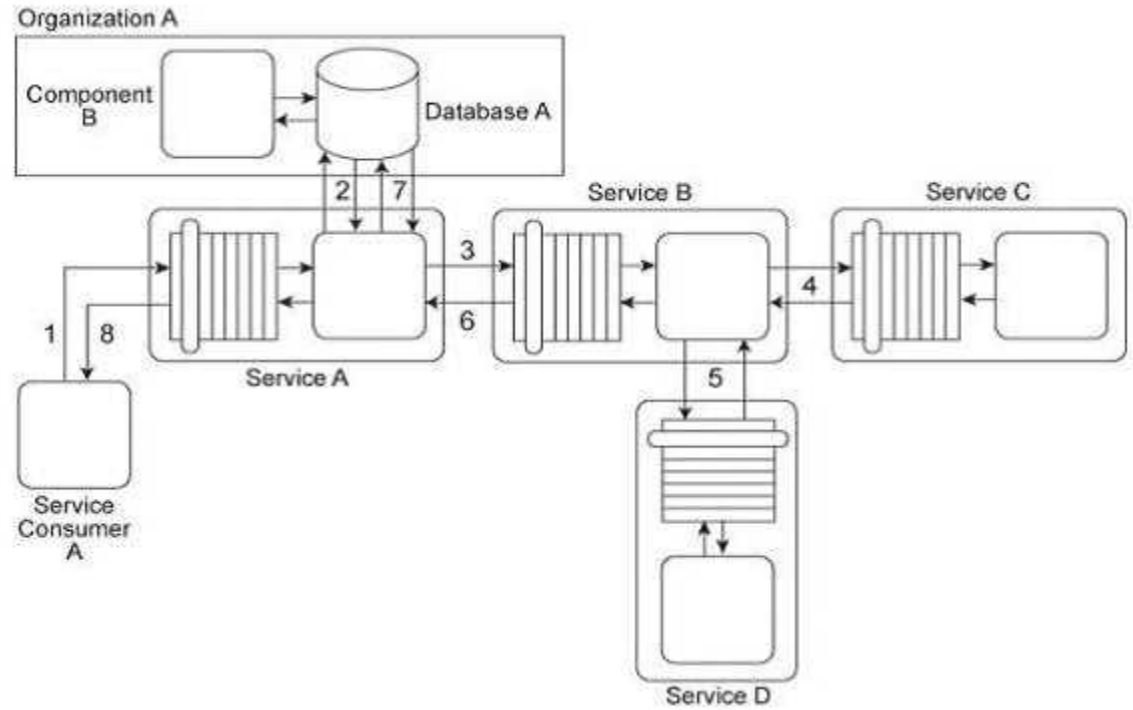
Thank you for Downloading S90-20A exam PDF Demo

You can also try our S90-20A Full Version Download

Download Free Demo:
https://www.certkillers.net/Exam/S90-20A

Question: 1

Service Consumer A sends a request message to Service A (1) after which Service A retrievesfinancial data from Database A (2). Service A then sends a request message with the retrieveddata to Service B (3). Service B exchanges messages with Service C (4) and Service D (5), whichperform a series of calculations on the data and return the results to Service A .Service A usesthese results to update Database A (7) and finally sends a response message to ServiceConsumer A (8). Component B has direct, independent access to Database A and is fully trustedby Database A .Both Component B and Database A reside within Organization A .ServiceConsumer A and Services A, B, C, and D are external to the organizational boundary ofOrganization A.



Component B is considered a mission critical program that requires guaranteed access to and fastresponse from Database A .Service A was recently the victim of a denial of service attack, whichresulted in Database A becoming unavailable for extended periods of time (which furthercompromised Component B). Additionally, Services B, C, and D have repeatedly been victims ofmalicious 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 forauthenticating all access to the database by Service A and any other service consumers. Due tothe mission critical requirements of Component B, the utility service further contains logic thatstrictly limits the amount of concurrent requests made to Database A from outside theorganizational boundary. The Data Confidentiality and Data Origin Authentication patterns areapplied to all message exchanged within the external service composition in order to establishmessage-layer security.
B. Service Consumer A generates a private/public key pair and sends this public key and identityinformation to Service A .Service A generates its own private/public key pair and sends it

back toService Consumer A .Service Consumer A uses the public key of Service A to encrypt a randomlygenerated session key and then sign the encrypted session key with the private key. Theencrypted, signed session key is sent to Service A .Now, this session key can be used for securemessage-layer communication between Service Consumer A and Service A .The ServicePerimeter Guard pattern is applied to establish a perimeter service that encapsulates Database Ain order to authenticate all external access requests.

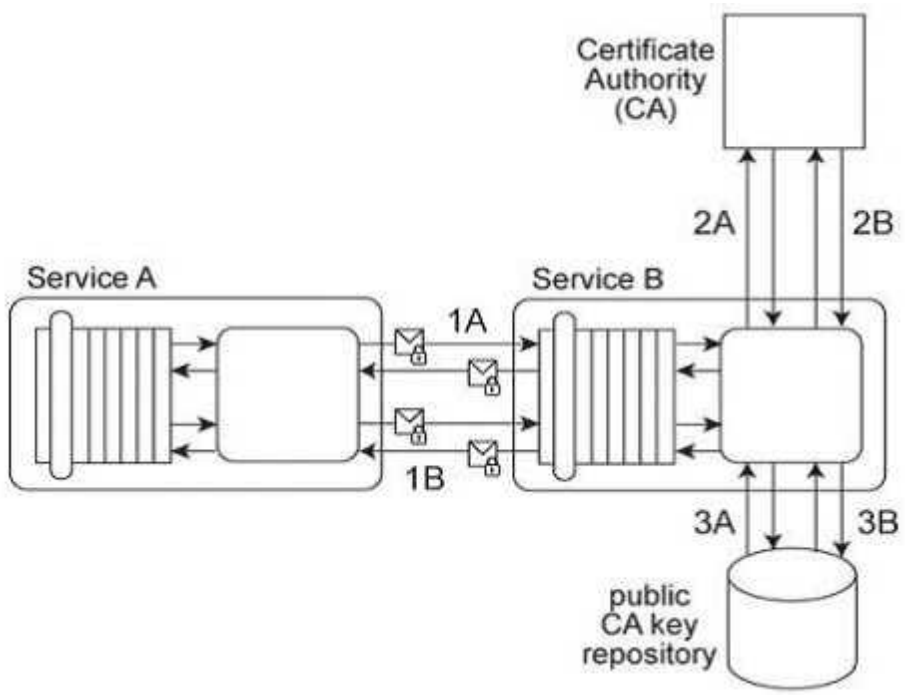
C. Services B, C, and D randomly generate Session Key K, and use this key to encrypt requestand response messages with symmetric encryption. Session Key K is further encrypted itselfasymmetrically. When each service acts as a service consumer by invoking another service, itdecrypts the encrypted Session Key K and the invoked service uses the key to decrypt theencrypted response. Database A is replicated so that only the replicated version of the databasecan be accessed by Service A and other external service consumers.

D. The Direct Authentication pattern is applied so that when Service Consumer A submits securitycredentials, Service A will be able to evaluate the credentials in order to authenticate the requestmessage. If the request message is permitted, Service A invokes the other services and accessesDatabase A .Database A is replicated so that only the replicated version of the database can beaccessed by Service A and other external service consumers.

Answer: A

Question: 2

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



To fulfill a new security requirement, Service A needs to be able to verify that the responsemessage sent by Service B has not been modified during transit. Secondly, the runtimeperformance between Services A and B has been unacceptably poor and therefore must beimproved without losing the ability to verify Service A's security credentials. It has beendetermined that the latency is being caused by redundant security processing carried out byService B .Which of the following statements describes a solution that fulfills these requirements?

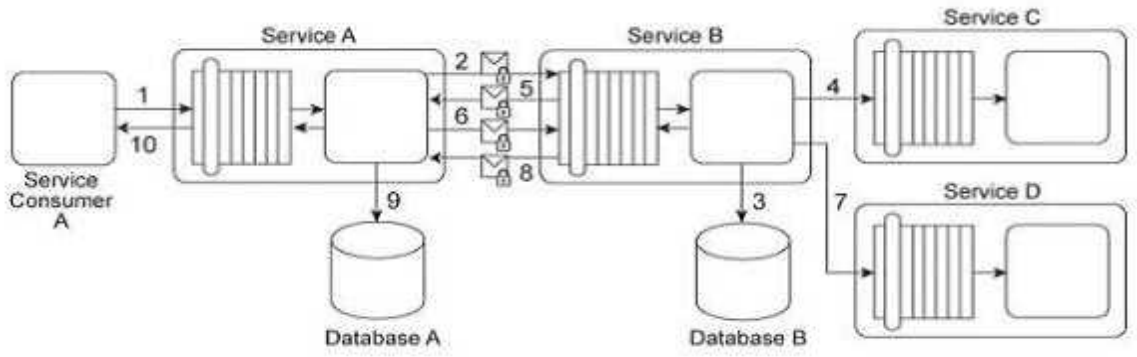
A. Apply the Trusted Subsystem pattern to introduce a utility service that performs the securityprocessing instead of Service B .The utility service can verify the security credentials of requestmessages from Service A and digitally sign messages sent to Service A to enable verification ofmessage integrity. Furthermore, the utility service can perform the verification of securitycredentials submitted by Service A only once per runtime service activity. After the firstmessage-exchange, it can issue a SAML token to Service A that gets stored within the currentsession. 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 isno 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 fromService A only for the first message exchange during the runtime service activity. Thereafter, it canissue a SAML token to Service A that gets stored within the current session. Service A then usesthis session-based token with subsequent message exchanges. Because SAML tokens have avery small validity period (in contrast to X.509 certificates), there is no need to perform arevocation check with every message exchange.
C. WS-Security-Policy transport binding assertions can be used to improve performance viatransport-layer security Tkhe use of symmetric keys can keep the encryption and decryptionoverhead 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 actionsfor integrity verification are needed.
D. The Data Origin Authentication pattern can be applied together with the Service PerimeterGuard pattern to establish a perimeter service that can verify incoming request messages sent toService B

and to filter response messages sent to Service A .The repository containing theverification information about the Certificate Authorities can be replicated in the trust domain of theperimeter service. When access is requested by Service A, the perimeter service evaluatessubmitted 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 hashvalue.

Answer: A

Question: 3

Service Consumer A sends a request message to Service A (1), after which Service A sends arequest message with security credentials to Service B (2). Service B authenticates the requestand, 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 aresponse message. Service B then sends a response message back to Service A (5). Afterprocessing Service B's response, Service A sends another request message with securitycredentials to Service B (6). After successfully authenticating this second request message fromService A, Service B sends a request message to Service D (7). Service D is also not required toissue a response message. Finally, Service B sends a response message to Service A (8), afterwhich Service A records the response message contents in Database A (9) before sending its ownresponse message to Service Consumer A (10).



Services A and B use digital certificates to support message integrity and authentication. Withevery message exchange between the two services (2, 5, 6, 8), the digital certificates are used. Ithas been determined that both Databases A and B are vulnerable to malicious attackers that maytry to directly access sensitive data records. Furthermore, performance logs have revealed that thecurrent 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 bemaintained, but with improved runtime performance - and - how can Databases A and B beprotected with minimal additional impact on performance?

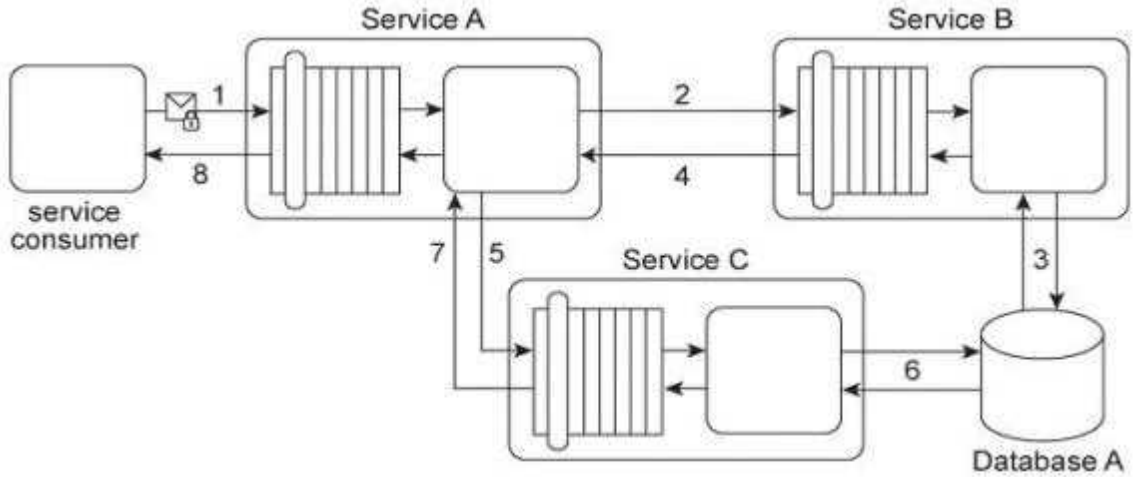
A. Apply the Brokered Authentication pattern to establish an authentication broker that uses WS-Trust based SAML tokens for message exchanges between Services A and B .This eliminates theneed for Service A to be repeatedly authenticated by Service B .Use the public key of Service A toencrypt Database 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-Secure-Conversation Security-context tokens (SCTs) to generate and transmit a symmetric sessionkey. The session key is used to encrypt and digitally sign messages exchanged between ServicesA and B .For each database the Trusted Subsystem pattern is applied to require

authenticatedaccess to the database and to prevent attackers from accessing the database directly
C. Apply the Direct Authentication pattern to establish mutual authentication between Services Aand B using a shared identity store. Service A attaches a Username token to the first requestmessage sent to Service B and Service B authenticates the request message using the sharedidentity store. Similarly, when Service B submits a response message to Service A .it attaches itsown 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 keyand 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 theneed for Service A to be repeatedly authenticated by Service B .Database A is encrypted usingthe Service A password as a secret encryption key and Database B is encrypted using the ServiceB password as a secret encryption key.

Answer: B

Question: 4

Service A provides a customized report generating capability. Due to infrastructure limitations, thenumber 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 authenticationof the request message is successful, Service A sends a message to Service B (2) to retrieve therequired data from Database A (3). Service A stores the response from Service B (4) in memoryand then issues a request message to Service C (5). Service C retrieves a different set of datafrom Database A (6) and sends the result back to Service A (7). Service A consolidates the datareceived from Services B and C and sends the generated report in the response message to itsservice consumer (8).



This service composition was recently shut down after it was discovered that Database A hadbeen successfully attacked twice in a row. The first type of attack consisted of a series ofcoordinated request messages sent by the same malicious service consumer, with the intention oftriggering a range of exception conditions within the database in order to generate various errormessages. The second type of attack consisted of a service consumer sending request messageswith malicious input with the intention of gaining control over the database server. This attackresulted in the deletion of

database records and tables. An investigation revealed that both attackswere carried out by malicious service consumers that were authorized.How can the service composition security architecture be improved to prevent these types ofattacks?

A. Apply the Data Confidentiality pattern together with the Data Origin Authentication pattern. Thisestablishes message-level-security so that all messages are encrypted and digitally signed.Secondly, the Service A logic must be enhanced so that it can keep track of the trustworthiness ofits service consumers If a request message originated from a trustworthy service consumer, thenthe request message is processed as normal. If the request message originates from a non-trustworthy service consumer, then the request message is rejected and an error message isreturned to the service consumer.
B. Apply the Service Perimeter Guard pattern together with the Trusted Subsystem pattern. Thisestablishes a perimeter service between Database A and any service that requires access to it(including Services B and C). The perimeter service evaluates incoming data requests and filtersout those that can introduce a security risk. Only request messages issued by authorized servicesand service consumers are forwarded to Database A .Responses originating from Database A arefurther evaluated by the trusted subsystem to remove any unauthorized data. The two patternstogether ensure that only authorized data is returned to the service consumer and that no requestmessages present a security threat to Database A.
C. Apply the Exception Shielding pattern together with the Message Screening pattern. Thisestablishes new logic within Service A that screens incoming request messages for data-drivenattacks (such as SQL injection and X-Path injection attacks), and also evaluates whether exceptiondetails returned by Database A contains potentially confidential or unsafe information. Anyinappropriate exception information is replaced with sanitized content.
D. Apply the Trusted Subsystem pattern to protect Database A from data-driven attacks and toevaluate whether database-responses contain inappropriate data. The trusted subsystemmaintains a snapshot of Database A and executes the original service consumer's requestmessage against the snapshot. The processing logic that accesses the snapshot has limitedprivileges in order to prevent malicious attacks from overtaking the database. If no securityviolation is detected during the processing of the snapshot, then the original service consumer'srequest is forwarded to Database A .If an error message is generated during the processing of thesnapshot, then it is returned to the original service consumer and the request is not forwarded toDatabase A .Because the error message was generated on the snapshot, it cannot contain unsafeinformation about Database A.

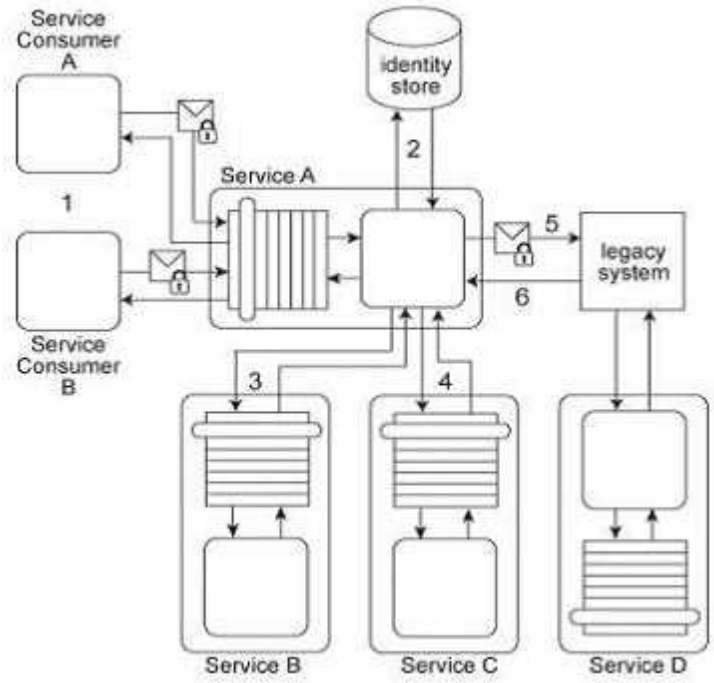
Answer: C

Question: 5

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 A .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 A .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

Thank You for trying S90-20A PDF Demo

To Buy Latest S90-20A Full Version Download visit link below

https://www.certkillers.net/Exam/S90-20A

Start Your S90-20A Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further 10% discount on your purchase. Test your S90-20A preparation with actual exam questions.