Google Discussions

Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

Go to Exam

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 19 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 19
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You need to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer. What should you do?

A. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the encrypted DEK.

B. Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the KEK.

C. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the encrypted DEK.

D. Generate a new data encryption key (DEK) in Cloud KMS to encrypt the data, and generate a key encryption key (KEK) locally to encrypt the key. Store both the encrypted data and the KEK.

Show Suggested Answer

by ArizonaClassics at *Aug. 2, 2020, 12:47 a.m.*

Comments

Type your comment...

Submit

Sheeda Highly Voted 4 years, 5 months ago

Yes, A is correct

The process of encrypting data is to generate a DEK locally, encrypt data with the DEK, use a KEK to wrap the DEK, and then store the encrypted data and the wrapped DEK. The KEK never leaves Cloud KMS.

upvoted 22 times

MohitA 4 years, 5 months ago

Agree on A, spot on "KEK never leaves Cloud KMS"

upvoted 3 times

Di4sa Most Recent 11 months, 1 week ago

Selected Answer: A

A is the correct answer as stated in google docs
The process of encrypting data is to generate a DEK locally, encrypt data with the DEK, use a KEK to wrap the DEK, and then store the encrypted data and the wrapped DEK. The KEK never leaves Cloud KMS.
https://cloud.google.com/kms/docs/envelope-encryption#how_to_encrypt_data_using_envelope_encryption

upvoted 2 times

standm 1 year, 8 months ago

KMS is used for storing KEK in CSEK & CMEK

upvoted 1 times

aashissh 1 year, 9 months ago

Selected Answer: B

This follows the recommended practice of envelope encryption, where the DEK is encrypted with a KEK, which is managed by a KMS service such as Cloud KMS. Storing both the encrypted data and the KEK allows for the data to be decrypted using the KEK when needed. It's important to generate the DEK locally to ensure the security of the key, and to generate a new KEK in Cloud KMS for added security and key management capabilities.

upvoted 1 times

ppandher 1 year, 3 months ago

We need to store the encrypted data and Wrapped DEK . KEK would be centrally Managed by KMS .
https://cloud.google.com/kms/docs/envelope-encryption#how_to_encrypt_data_using_envelope_encryption

upvoted 1 times

GCP72 2 years, 5 months ago

Selected Answer: A

The answer is A

upvoted 2 times

minostrozaml2 3 years ago

Took the tesk today, only 5 question from this dump, the rest are new questions.

upvoted 1 times

Bill831231 3 years, 1 month ago

A sounds like the correct answer:
https://cloud.google.com/kms/docs/envelope-encryption#how_to_encrypt_data_using_envelope_encryption

upvoted 1 times

umashankar_a 3 years, 6 months ago

Answer A
Envelope Encryption: https://cloud.google.com/kms/docs/envelope-encryption
Here are best practices for managing DEKs:
-Generate DEKs locally.
-When stored, always ensure DEKs are encrypted at rest.
- For easy access, store the DEK near the data that it encrypts.
The DEK is encrypted (also known as wrapped) by a key encryption key (KEK). The process of encrypting a key with another key is known as envelope encryption.
Here are best practices for managing KEKs:
-Store KEKs centrally. (KMS)
-Set the granularity of the DEKs they encrypt based on their use case. For example, consider a workload that requires multiple DEKs to encrypt the workload's data chunks. You could use a single KEK to wrap all DEKs that are responsible for that workload's encryption.
-Rotate keys regularly, and also after a suspected incident.

upvoted 2 times

desertlotus1211 3 years, 9 months ago

I'm no sure what the answers is, but the answers to this question has changed.... be prepared

upvoted 1 times

dtmtor 3 years, 10 months ago

Answer is A

upvoted 1 times

DebasishLowes 3 years, 10 months ago

Ans : A

upvoted 1 times

CloudTrip 3 years, 11 months ago

Correction I change it to A after reading the question once again.

upvoted 1 times

CloudTrip 3 years, 11 months ago

Answer is B as after DEK encryption it's KEK (not encrypted DEK) which never leaves KMS

upvoted 1 times

Bharathy 4 years, 1 month ago

A - Envelope Encryption (DEK - to encrypt the data, KEK - encrypt the DEK , KEK resides in KMS and only the encrypted data and wrapped DEK will be stored back)

upvoted 2 times

CHECK666 4 years, 4 months ago

The answer is A

upvoted 1 times

aiwaai 4 years, 5 months ago

The Answer is A

upvoted 2 times

ArizonaClassics 4 years, 5 months ago

C is the correct option. See BEST Practices for managing DEKS
https://cloud.google.com/kms/docs/envelope-encryption

upvoted 1 times

ArizonaClassics 4 years, 5 months ago

A is the correct one. Made a mistake earlier

upvoted 2 times

kumar999 4 years, 5 months ago

It is A. See How to encrypt data using envelope encryption

upvoted 2 times

ArizonaClassics 4 years, 5 months ago

Thank you Kumar. it is A. I made a mistake.

upvoted 1 times