

🔗 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 45 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 45

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

A large financial institution is moving its Big Data analytics to Google Cloud Platform. They want to have maximum control over the encryption process of data stored at rest in BigQuery.

What technique should the institution use?

- A. Use Cloud Storage as a federated Data Source.
- B. Use a Cloud Hardware Security Module (Cloud HSM).
- C. Customer-managed encryption keys (CMEK).
- D. Customer-supplied encryption keys (CSEK).

[Show Suggested Answer](#)

by [jonclem](#) at March 26, 2020, 6:11 p.m.

Comments

Type your comment...

[Submit](#)

🗨️ [Ganshank](#) [Highly Voted](#) 5 years, 2 months ago

CSEK is only supported in Google Cloud Storage and Compute Engine, therefore D cannot be the right answer. Ideally, it would be client-side encryption, with BigQuery providing another round of encryption of the encrypted data -

really, it would be client side encryption, with BigQuery providing another round of encryption of the encrypted data
https://cloud.google.com/bigquery/docs/encryption-at-rest#client_side_encryption, but since that is not one of the options, we can go with C as the next best option.

👍 🔄 🚩 upvoted 19 times

🗳️ 👤 **smart123** 5 years, 1 month ago

Option 'C' is correct. Option 'D' is not correct as CSEK a feature in Google Cloud Storage and Google Compute Engine only.

👍 🔄 🚩 upvoted 5 times

🗳️ 👤 **Zek** Most Recent 7 months, 4 weeks ago

Selected Answer: C

BigQuery and BigLake tables don't support Customer-Supplied Encryption Keys (CSEK).
https://cloud.google.com/bigquery/docs/customer-managed-encryption#before_you_begin

👍 🔄 🚩 upvoted 3 times

🗳️ 👤 **SQLbox** 10 months, 3 weeks ago

Correct answer is b

👍 🔄 🚩 upvoted 1 times

🗳️ 👤 **crazycosmos** 12 months ago

Selected Answer: D

I prefer D for max control.

👍 🔄 🚩 upvoted 1 times

🗳️ 👤 **SQLbox** 1 year ago

Correct answer is D

D. Customer-supplied encryption keys (CSEK).

Here's an explanation of why CSEK is the best choice and a brief review of the other options:

Customer-supplied encryption keys (CSEK): CSEK allows the institution to manage their own encryption keys and supply these keys to Google Cloud Platform when needed. This provides maximum control over the encryption process because the institution retains possession of the encryption keys and can rotate, revoke, or replace them as desired.

👍 🔄 🚩 upvoted 1 times

🗳️ 👤 **Ishu_awsguy** 2 years, 1 month ago

Why not Cloud HSM ?
Maximum control over keys

👍 🔄 🚩 upvoted 1 times

🗳️ 👤 **Ishu_awsguy** 2 years, 1 month ago

Sorry

From HSM the keys become customer supplied encryption keys which are not supported.

Ans is Customer managed encryption keys

👍 🔄 🚩 upvoted 1 times

🗳️ 👤 **AwesomeGCP** 2 years, 9 months ago

Selected Answer: C

C. Customer-managed encryption keys (CMEK).

👍 🔄 🚩 upvoted 3 times

🗳️ 👤 **DebasishLowes** 4 years, 4 months ago

Ans : C

👍 🔄 🚩 upvoted 2 times

🗳️ 👤 **Aniyadu** 4 years, 6 months ago

I feel C is the right answer. if customer wants to manage the keys from on-premises then D would be correct.

👍 🔄 🚩 upvoted 3 times

🗳️ 👤 **saarabh1805** 4 years, 9 months ago

C is correct answer as CSEK is not available for big query.

👍 🔄 🚩 upvoted 3 times

🗳️ 👤 **MohitA** 4 years, 11 months ago

C is the right answer as CSEC is only available for CS and CE's

👍 🔄 🚩 upvoted 1 times

🗳️ 👤 **aiwaai** 4 years, 11 months ago

Correct Answer: C

👍 ↩ 🚩 upvoted 2 times

🗄 👤 **ArizonaClassics** 4 years, 11 months ago

C is the RIGHT ONE!!!

If you want to manage the key encryption keys used for your data at rest, instead of having Google manage the keys, use Cloud Key Management Service to manage your keys. This scenario is known as customer-managed encryption keys (CMEK).

<https://cloud.google.com/bigquery/docs/encryption-at-rest>

👍 ↩ 🚩 upvoted 2 times

🗄 👤 **ArizonaClassics** 4 years, 11 months ago

ALSO READ : <https://cloud.google.com/bigquery/docs/customer-managed-encryption>

👍 ↩ 🚩 upvoted 2 times

🗄 👤 **ranjeetpatil** 5 years, 1 month ago

Ans is C. BigQuery does not support CSEK. <https://cloud.google.com/security/encryption-at-rest>.

<https://cloud.google.com/security/encryption-at-rest>

👍 ↩ 🚩 upvoted 4 times

🗄 👤 **srinidutt** 5 years, 2 months ago

I also feel D is right

👍 ↩ 🚩 upvoted 1 times

🗄 👤 **xhova** 5 years, 3 months ago

Answer is D. For max control you don't want to store the Key with Google.

👍 ↩ 🚩 upvoted 3 times

🗄 👤 **jonclem** 5 years, 4 months ago

For maximum control surely D is the correct answer.

CSEK:

<https://cloud.google.com/security/encryption-at-rest/customer-supplied-encryption-keys>

CMEK

<https://cloud.google.com/bigquery/docs/encryption-at-rest>

👍 ↩ 🚩 upvoted 2 times



Platform

> Home

> All Exams

> Examtopics PRO

> Training Courses

