Google Discussions

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 151 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 151
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your privacy team uses crypto-shredding (deleting encryption keys) as a strategy to delete personally identifiable information (PII). You need to implement this practice on Google Cloud while still utilizing the majority of the platform's services and minimizing operational overhead. What should you do?

A. Use client-side encryption before sending data to Google Cloud, and delete encryption keys on-premises.

B. Use Cloud External Key Manager to delete specific encryption keys.

C. Use customer-managed encryption keys to delete specific encryption keys.

D. Use Google default encryption to delete specific encryption keys.

Show Suggested Answer

by Random_Mane at *Sept. 17, 2022, 6:17 p.m.*

Comments

Type your comment...

Submit

Random_Mane Highly Voted 10 months, 2 weeks ago

Selected Answer: C

C. https://cloud.google.com/sql/docs/mysql/cmek
"You might have situations where you want to permanently destroy data encrypted with CMEK. To do this, you destroy the customer-managed encryption key version. You can't destroy the keyring or key, but you can destroy key versions of the key."

upvoted 11 times

AzureDP900 Most Recent 8 months, 4 weeks ago

C is right

upvoted 2 times

rotorclear 9 months, 2 weeks ago

Selected Answer: C

CMEK allows users to manage their keys on google without operation overhead of managing keys externally

upvoted 4 times

AwesomeGCP 9 months, 3 weeks ago

Selected Answer: C

C. Use customer-managed encryption keys to delete specific encryption keys.

upvoted 2 times

zellck 10 months ago

Selected Answer: C

C is the answer to minimise operational overhead.

upvoted 3 times