◉ **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 237 DISCUSSION**

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 237

Topic #: 1

**[All Professional Cloud Security Engineer Questions]**

Your organization wants full control of the keys used to encrypt data at rest in their Google Cloud environments. Keys must be generated and stored outside of Google and integrate with many Google Services including BigQuery.

What should you do?

A. Use customer-supplied encryption keys (CSEK) with keys generated on trusted external systems. Provide the raw CSEK as part of the API call.

B. Create a KMS key that is stored on a Google managed FIPS 140-2 level 3 Hardware Security Module (HSM). Manage the Identity and Access Management (IAM) permissions settings, and set up the key rotation period.

C. Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors.

D. Create a Cloud Key Management Service (KMS) key with imported key material. Wrap the key for protection during import. Import the key generated on a trusted system in Cloud KMS.

**Show Suggested Answer**

by ⊙ **MisterHairy** at *Nov. 21, 2023, 10:58 p.m.*

## Comments

Type your comment...

|  | Submit |

☐ 👤 **Pime13** 7 months, 3 weeks ago

**Selected Answer: C**

https://cloud.google.com/assured-workloads/docs/overview

👍 ↩ 🏳 upvoted 1 times

☐ 👤 **Mr_MIXER007** 10 months, 3 weeks ago

**Selected Answer: C**

Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors

👍 ↩ 🏳 upvoted 1 times

☐ 👤 **AgoodDay** 11 months, 2 weeks ago

**Selected Answer: C**

agree with c

👍 ↩ 🏳 upvoted 1 times

☐ 👤 **Bettoxicity** 1 year, 3 months ago

**Selected Answer: C**

C.
-Full Key Control: Cloud EKM allows you to leverage an external HSM, providing complete control over key generation and storage outside of Google's infrastructure. This satisfies your organization's key control requirement.
-Google Service Integration: Cloud EKM integrates seamlessly with numerous Google Services, including BigQuery. You can use these external keys for encrypting data at rest within those services.

👍 ↩ 🏳 upvoted 1 times

☐ 👤 **dija123** 1 year, 4 months ago

**Selected Answer: C**

Agree with C

👍 ↩ 🏳 upvoted 1 times

☐ 👤 **NaikMN** 1 year, 7 months ago

C
https://cloud.google.com/kms/docs/ekm

👍 ↩ 🏳 upvoted 1 times

☐ 👤 **MisterHairy** 1 year, 8 months ago

**Selected Answer: C**

The correct answer is C. Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors.

Cloud EKM allows you to use encryption keys that are stored and managed in a third-party key management system deployed outside of Google's infrastructure. This gives your organization full control over the keys used to encrypt data at rest in Google Cloud environments, including BigQuery.

👍 ↩ 🏳 upvoted 1 times