Hold Your Own Key (HYOK)

Last Modified on 10/22/2024 4:59 pm IDT

This article is designated for administrators.

About

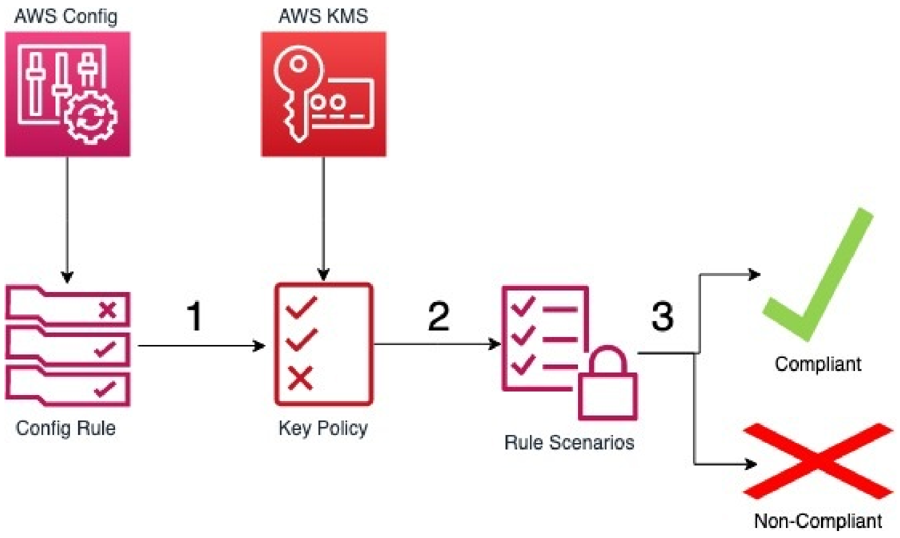
Hold Your Own Key (HYOK) is a security model where clients generate, manage, and store their own encryption keys, ensuring full control over the encryption and decryption of their data. In this model, the service providers, i.e. Kaltura, in this case, never have access to the encryption keys, allowing clients to maintain maximum privacy and data security.

HYOK flow

1. The client should manage their own keys using AWS Key Management Service (KMS). Here you can:
    - Centrally create, view, edit, monitor, enable or disable, rotate, and schedule deletion of KMS keys.
    - Define the policies that control how and by whom KMS keys can be used.
    - Audit the usage to prove that it is being used correctly. Auditing is supported by the AWS KMS API, but not by the AWS Management Console.

2. The client should assign Kaltura permissions to the key via an AWS IAM Role with the option to use grants. To learn more, see Authentication and Access Control for AWS KMS.

Authentication and access control for AWS KMS

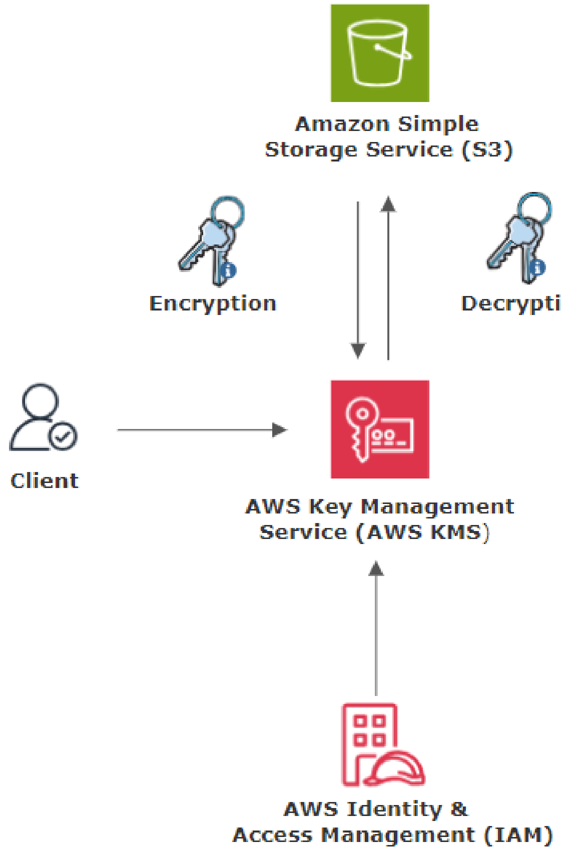


For more information, see AWS Key Management Service , and AWS KMS concepts.

3. Kaltura will manage a dedicated S3 bucket for the client. Using the IAM role, Kalutra gets permission to the encrypted key and the S3 bucket. To learn more, see Amazon IAM - Identity and Access Management.

   ⚠ If the client decides to revoke access to the Key (essentially revoking the IAM role they gave us), everything remains encrypted and essentially inaccessible to Kaltura or anyone with access to the S3 bucket.

This architecture allows the client to have full control of encryption and decryption operations, minimizing the security risks associated with storing and processing sensitive data in the cloud. The client can also use AWS monitoring to see who accessed the key and when.


Amazon Simple Storage Service (S3)
Encryption
Decryption
Client
AWS Key Management Service (AWS KMS)
AWS Identity & Access Management (IAM)

Prerequisites & setup

1. Customers must obtain an AWS Account, manage their own AWS KMS keys, and assign Kaltura permissions to the key via an AWS IAM Role with the option to use grants.
2. The full HYOK implementation is being set up by Kaltura Professional Services.

To learn more, see HYOK datasheet_1.pdf or contact your Kaltura representative.