Zoom Customer Managed Key

WHITEPAPER

Introduction

The purpose of this document is to provide an overview of the product architecture and deployment options of Zoom Customer Managed Key (CMK), Zoom's Bring Your Own Key (BYOK) solution or more specifically, Hold Your Own Key (HYOK) solution.

The goal of Zoom Customer Managed Key is to help customers protect select data stored at rest within the Zoom Cloud infrastructure using their own encryption keys managed by a Key Management Service (KMS) of their choice.

Why use a BYOK (or HYOK) solution?

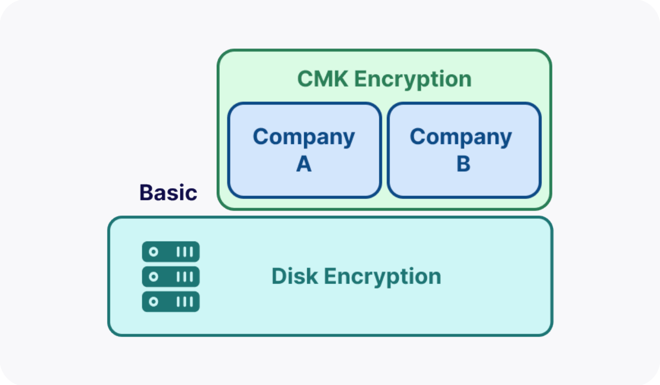
There are several different use cases for why a customer may need a BYOK solution:

- **Meeting compliance requirements:** Every industry grapples with its own unique regulatory requirements — the healthcare industry faces HIPAA, while financial services institutions must address Gramm-Leach Bliley Act, NY DFS, and more. All organizations have a different approach to safeguarding important information and aligning with their compliance obligations (or internal policies), and some (such as Cloud Computing Compliance Criteria Catalog, known as C5) need tailored security solutions like a BYOK solution to do so.
- **Approximating data residency:** The evolving regulatory and legal landscape can be supported by allowing customers to control encryption keys in a specific geographic region if the data protected by the keys resides in a different region. A BYOK solution helps support data sovereignty and data residency requirements by giving control over how and where those keys are accessed.
- **Managing risk:** Some customers have risk management postures from their security organization that require protecting and monitoring data stored in vendor clouds with their own encryption keys. A BYOK solution gives customers additional transparency and control over their data at rest.

The following document outlines the current scope of Zoom's HYOK solution, the encryption and decryption process, as well as guidance for deploying Zoom Customer Managed Key for your organization.

Solution overview

Collaboration now occurs across several mediums and communication channels, and Zoom is committed to meeting our customers where they are and keeping their data protected. Since we handle the communication needs of many companies, we also maintain customer data like meeting recordings and phone voicemails. Certain customer data, including cloud recordings, chat history, and meeting transcripts are stored at-rest in the Zoom cloud infrastructure using 256-bit AES-GCM encryption. These objects are encrypted with a uniquely generated key, managed by a key management system (KMS) in the cloud.



Zoom Customer Managed Key is a new infrastructure service that gives customers additional transparency and control to protect certain data at rest. The data is still encrypted at rest, but specific Zoom services also encrypt the data objects using a key provided by the customer. This creates a second layer of encryption and currently does not replace the standard encryption that Zoom data at rest uses. (In the future, some new assets may only get encrypted using the customer provided key)

Zoom Customer Managed Key (CMK) allows an organization to retain control and management of keys used to encrypt their data at-rest within Zoom's infrastructure using envelope encryption, which is described in more detail below. Instead of using an encryption key generated and managed by Zoom's KMS, certain data is encrypted additionally when stored at-rest using a key generated and managed by the customer's KMS. This separation of duties allows customers to audit data at-rest access requests made via Zoom, and manage access to data at-rest at any time by revoking key access.

Zoom assets available for encryption

With Zoom Customer Managed Key, customers can opt to use their own encryption keys to encrypt certain Zoom assets stored at-rest. The list of assets[1] they can select from includes (as of April 2023):

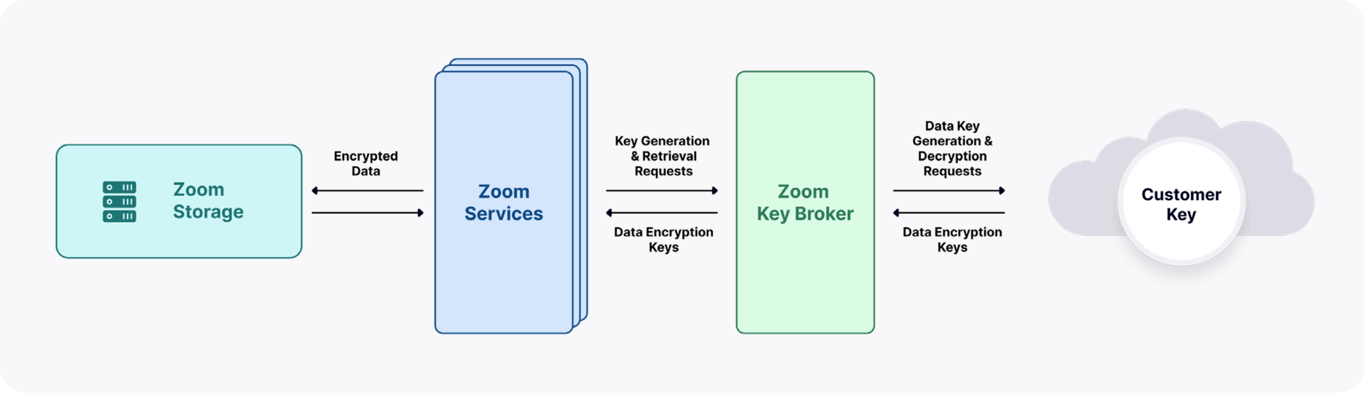
- Zoom Meeting cloud recordings (including transcripts, summaries, and chat texts unless those are shared with Team Chat)
- Zoom Webinars cloud recordings
- Zoom Phone voicemails and recordings (including transcripts) and MMS messages
- Zoom Team Chat internal messages (includes emojis, attached files including code snippets, but not reaction emojis or giphys as they are only referenced)
- Zoom Whiteboard drawings, text, pictures, and comments
- Zoom Clips videos
- Calendar access tokens for Zoom Rooms
- User calendar access tokens
- Microsoft Teams access tokens
- Archiving for meetings and webinars

For the most current list of assets, please refer to the support article.

Key management service requirement

Customers will need a key management service solution to oversee, automate, and secure the key management process with Zoom Customer Managed Key. Currently, Zoom supports customers who use AWS Key Management Service (AWS KMS), Microsoft's Azure Key Vault, or Oracle Cloud Infrastructure (OCI) Vault as their key management service. This means that customers will create their encryption keys in AWS, Azure, or OCI and grant access to Zoom Customer Managed Key for encrypting and decrypting Zoom assets. Many KMSes also allow customers to control key rotation and get transparency on how their keys were accessed by Zoom or use dedicated or even external high security modules. In the future, Zoom plans to offer support for additional key management service providers.

Solution architecture



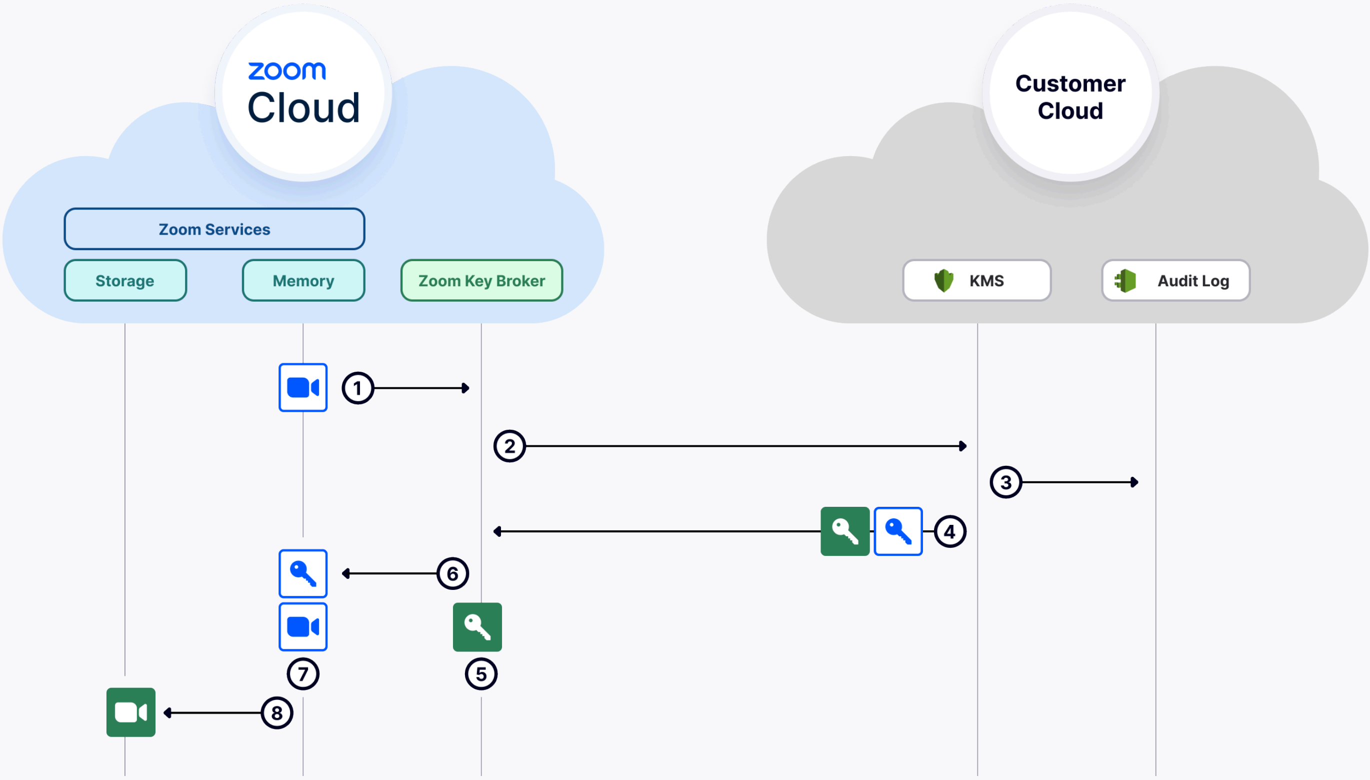
There are three major components involved:

Zoom services: This includes services such as the Zoom Meetings Service and Zoom Phone Services. These services are processing data in the Zoom Cloud Infrastructure and are creating data that needs to be stored.

Zoom key broker: The central component of Zoom Customer Managed Key is the Zoom key broker service. The key broker tracks whether an organization has enabled CMK, who its users are, what services they have enabled for encryption, and how to access the organization's key. To meet the scalability and high availability requirements of the Zoom cloud, the key broker service utilizes Zoom's Kubernetes and the message-based, on-demand infrastructure in each of our data centers to provide its services.

Key management service (KMS): The KMS securely generates, stores, and rotates the encrypting key and generates, encrypts, and decrypts data keys on behalf and under the control of the customer.

[1] Associated metadata, such as used for searching, may not be encrypted with the customer's key

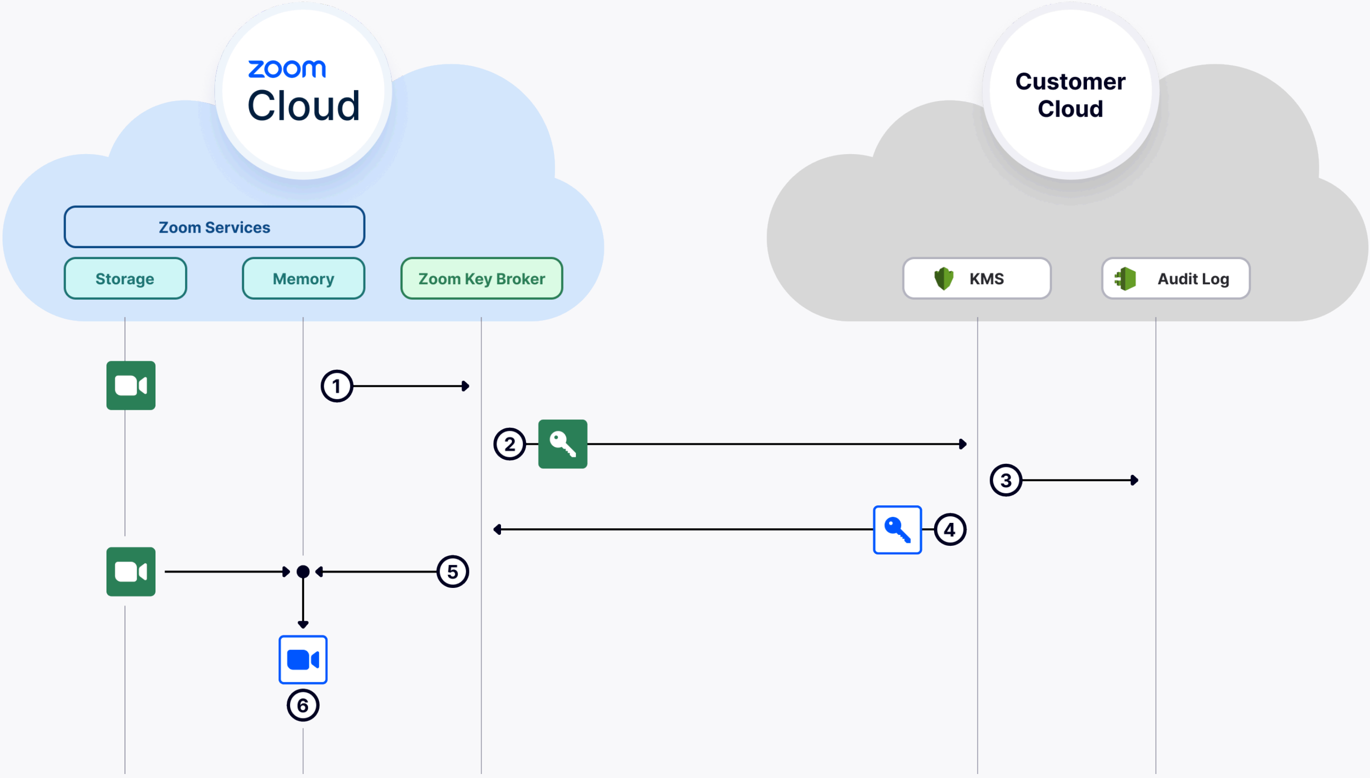


Encryption process

The above figure provides an example flow for how a meeting recording is encrypted using Zoom Customer Managed Key. The steps are as follows:

1. A user initiates a cloud recording (blue) and the meeting service calls the Zoom key broker, which makes an API request.
2. This request is forwarded to the customer's KMS over TLS for a new data key for a particular meeting. The KMS generates a unique data key for the object and encrypts it with the customer's KMS key.
3. The KMS then logs the request made by Zoom together with the meeting ID.
4. The KMS then returns the encrypted and plaintext data keys to the key broker over TLS.
5. The key broker retains the encrypted key with its meeting ID in a database.
6. The key broker returns the plaintext data key to the meeting service.
7. The meeting service uses the plaintext data key to encrypt the cloud recording.
8. Then the cloud recording is stored at rest (green).

After all files are stored, the meeting service discards the plaintext key from memory and can no longer access the recording without requesting a decryption key from the key broker.



Decryption process

The above figure provides an example flow for how a meeting recording is decrypted. The steps are as follows:

1. Once a user initiates access to the recording (green), the meeting service contacts the Zoom key broker to look up the encrypted key for the particular meeting.
2. The key broker sends the encrypted key to the customer's KMS over TLS for the plaintext version of the encrypted key associated with the object.
3. The customer's KMS decrypts the key and logs the request.
4. The KMS then returns the plaintext key over TLS to the key broker. (The key broker also caches the data key in encrypted memory for 5 minutes in case the user needs to access the recording again.)
5. The key broker forwards the plaintext key to the meeting service.
6. The meeting service uses the key to decrypt the recording (blue). It then sends the recording to the user and discards the data key from temporary memory.

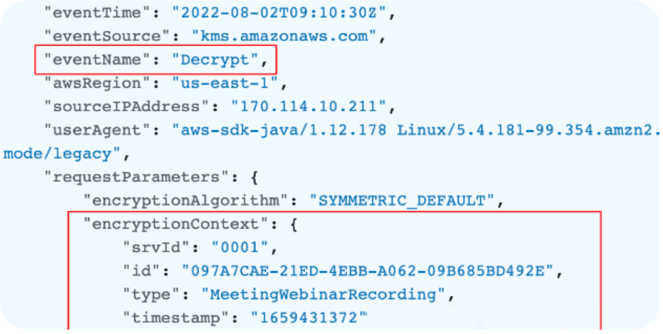
Auditing and monitoring

As the customer maintains their own KMS key and usually the KMS provides for audit logs, customers have an independent party provide detailed logs. By default, any AWS KMS key operation such as key creation and rotation will be logged in CloudTrail. This includes the requests by the Zoom key broker to generate a data key for encryption or retrieve a data key for decryption but does not include any decryption requests which were handled by the key broker's cache.

Log entries include basic information like event type, time, and region. For each enabled Zoom service the Zoom key broker provides additional encryption context for the log such as:

- srvId: The identifier of the service, e.g. 1 for Meeting Recorder
- type: The type of the asset, e.g. "MeetingWebinarRecording"
- ID: The identifier within the service, e.g. the meeting number
- timestamp: UNIX timestamp

The detailed log may allow an internal auditing of access to resources.



```
    "eventTime": "2022-08-02T09:10:30Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "170.114.10.211",
    "userAgent": "aws-sdk-java/1.12.178 Linux/5.4.181-99.354.amzn2.
mode/legacy",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "encryptionContext": {
            "srvId": "0001",
            "id": "097A7CAE-21ED-4EBB-A062-09B685BD492E",
            "type": "MeetingWebinarRecording",
            "timestamp": "1659431372"
```

Log history can be maintained in AWS S3 storage and the admin can set alarms in AWS CloudWatch if necessary when suspicious behavior is detected.

Key access restrictions

While Zoom provides access control through various user management and passcode features, Zoom CMK provides organizations another level of transparency and control. If at any point the organization would like to restrict access to the data we store on their behalf, they can disable the KMS key or restrict the decryption of certain assets by restricting key access in general or selectively based on the encryption context.

If the key is disabled or encryption access is disabled, the services the customer had enabled for CMK will not be able to function anymore, for example recordings or chat will fail unless CMK is disabled for those services.

For more detailed information about how AWS KMS uses the encryption context, read this AWS security blog.

Deployment of Zoom Customer Managed Key

Each organization is responsible for the management of its own key in its own cloud account, enabling Zoom CMK in the Zoom Admin Portal, and monitoring the status of their encryption keys. We recommend a few best practices to further customize how keys are configured either directly by the customer or by Zoom's Professional Services Organization (PSO).

Key configuration

The first step is to create an encryption key in AWS KMS, Azure Key Vault, or OCI Vault. To avoid latency, the key should be created in the same data center as is configured for Zoom data storage (AWS US East by default).

While AWS KMS (and OCI Vault) already replicate each key to multiple availability zones, we encourage AWS customers to use AWS' multi-region key (MRK) option to replicate the key across multiple regions in some of the data centers in which Zoom operates for extra fault tolerance. Next, the organization needs to add the Zoom key broker to the key policy to give the Zoom key broker access to the keys.

While most organizations will rely on AWS's Automated key management for key rotation, organizations that need more control over key rotation and revocation can also use *Manual key management or External hardware security module*. OCI Vault provides similar options.

AUTOMATED KEY MANAGEMENT WITH AWS KMS

An admin can initiate automated key management with a few steps:

1. Create a new symmetric multi-region-key (MRK) in the AWS portal and enable auto key rotation.
2. Create a key policy configuration to give Zoom key broker access to the new key.
3. Specify the regions in AWS to replicate the key to by choosing regions where Zoom is already present.
4. Enter the key ID ARN (Amazon Resource Name) of the key in the Zoom Customer Managed Key section in the Zoom Admin Center.

No further configuration should be necessary as AWS KMS takes care of periodic key rotation, which is annual by default. From there,

1. New key material is created.
2. Material is automatically replicated to all configured regions.
3. The new material gets enabled for encryption while a history of old key material is maintained to allow for decryption of prior assets.

While the key material may change, the key's ID and policy stays the same. When the KMS generates a new data key, it returns the data key not only in plaintext, but also encrypts it for later retention as a cipherkey. The cipherkey contains the version ID of the key material to select the proper key material for decryption even if the key has been rotated in the meantime. This automates most key management tasks, but it does not allow for key deletion or deactivation of specific key materials.

MANUAL KEY MANAGEMENT

For more control, an organization can use manual rotation of their encryption keys. They will initially set up the first key as described above. Once they want to manually rotate or deactivate the key, they create a second key on the AWS portal and rotate/configure the new ARN in the Zoom admin portal. Once a new key has been configured, encryption access to any prior key may be revoked on the AWS portal though decryption access should still be maintained. The key broker will still use any prior keys to access and decrypt assets until any such prior key is disabled or deleted from the AWS portal.

EXTERNAL HARDWARE SECURITY MODULE (HSM)

If an organization prefers to generate and manage its own keys, it can set up its own HSM and upload the key material to a key in AWS KMS or use AWS External Key Store (XKS) to enable the Zoom key broker to access the HSM directly.

Switching key storage

Most KMSes offer the option to store keys either with their KMS directly or in an HSM they provide for customers. If an organization had started with a cloud KMS key and wants to use an HSM or switch between cloud providers, they can rotate the key to a new key in the new storage location. New assets will get encrypted using the new key management provider, but the old keys need to stay available to allow for decryption of existing assets until such access is not desired anymore.

Fallback control in case of key access issues

Access to the customer's key at all times is critical to create and access any content which has been selected to be secured by CMK. Zoom not only encourages the use of replicated keys, but also supports a global encryption "fallback control" option. If enabled and the customer's key is not available for encryption for any reason, CMK falls back to a Zoom provided backup key for encryption.

If neither key is available, content will not be stored. Zoom Phone even provides an option not only to fail recordings but drop a phone call in case no key is available for encryption.

During a fallback situation the key broker continues to reestablish access to the customer's key and once the problem has been resolved, CMK will re-encrypt all content with the customer's key.

Fallback control does not affect decryption and therefore content access though. If the key which was used to encrypt the content is unavailable, then the content cannot be retrieved, watched, or listened to.

Zoom admin portal

CONFIGURING KEYS

Zoom Customer Managed Key is available to customers if they have licensed either Zoom One Enterprise Plus or the Zoom Customer Managed Key add-on license. Once licenses have been purchased and the key is set up in the KMS, the administrator can configure Customer Managed Key in the "security" section of the Zoom admin portal and provide the following information:

1. Select the KMS provider (AWS, Azure, or OCI) and provide the key identifier
2. Assign licenses to the entire account or groups of users
3. Select which Zoom assets (meeting recordings, voicemails, chat etc.) will be encrypted
4. Supply the contact information (email address) to be notified if there are any issues with the key access
5. Enable fallback (optionally)

MONITORING KEYS

In the Zoom admin portal, admins can check which keys are in use, when they were last accessed or when access has failed for any reason. Admins can configure who gets notified if there are any key access issues or fallback gets triggered.

For details, see Using Customer Managed Key – Zoom Support

Conclusion

With half a million businesses choosing Zoom, protecting these users and their data is core to our goal to be a platform built on trust. Zoom Customer Managed Key is a solution that gives customers additional controls to use our platform according to their unique compliance requirements and data residency needs. This offering is built upon the same security and reliability as the rest of our platform, helping people communicate safely without sacrificing ease of use or productivity.

For more information, visit our Zoom Customer Managed Key webpage, and to get support implementing CMK, please contact Zoom Global Services.