2025 Cryptography Engineering

Google Client-Side Encryption

Final Project Topic

11 April, 2025

Outline

1. What is Google CSE
2. Critical Mechanism in Google CSE
3. Procedure of Google CSE
4. Advantage of Google CSE
5. Limitations of Google CSE
6. CSE v.s. E2E
7. Final Project’s Topics

1. What is Google CSE

Google CSE is a security function offered by Google Workspace, which make user can encrypt their data in local before uploading it to the Google server(cloud side).

Under CSE, the attacker cannot decrypt the data when he/she gets access to the server’s DB because “Google doesn’t stores the KEY”.

2. Critical Mechanism in Google CSE

a. Client-Side Encryption

- AES-GCM (data protection)
- RSA or EC (key protection)

e.g. When user upload a document to Google drive, Google drive will store the encrypt version rather than the raw data.

b. Key Management Service

- Google Cloud KMS or third-party KMS(AWS KMS\Microsoft Azure Key Vault)
- Only authorized user can access the “KEY”, Google service can’t access it

e.g. A company used a key to encrypt the document and store the document in Google drive. But the key is stored in AWS KMS.

c. Client-Side Decryption

- User authorization(OAuth 2.0)
- Zero trust access

e.g. Use OAuth 2.0 with Zero trust policy to management the user’s access right.

3. Procedure of Google CSE

Upload(encryption)

1. User choose a file to upload
2. Browser or local app use AES-GCM to encrypt data with its private key
3. Encrypt the private key with the “KMS public key”
4. Upload the encrypted data and encrypted private to Google server(cloud)

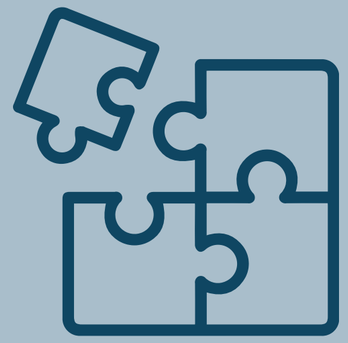
Download(descryption)

1. User request to download the encrypted data
2. Google send the encrypted data to user without decrypt method
3. User’s browser or local app send request to KMS for “KMS secret key”
4. If user is authorized, KMS will send the secret key.
5. Browser or app decrypt the data after decrypt the private with “KMS secret key”

4. Advantage of Google CSE

Compliance Requirements

- GDRR
- HIPAA
- FIPS



Flexible Key Management

- Support third-party KMS
- Management key by users

Private Protection

- Google or cloud operator can’t access data
- Attacker can’t get data from server directly

5. Limitations of Google CSE

Complexity

User need more steps to do KMS operation or encryption

Functions Limitations

Some Google service(search, suggestion) may not work under encryption data.

Key Management

The organization is responsible for managing the keys. If the keys are lost, the data cannot be recovered.

6. CSE v.s. E2E

Properties	CSE	E2E
Encrypt at	UE	UE
Key Management	Third-party (KMS)	User
Cloud Decryption	No	No
Applicable Scenarios	Company or Organization	Self-communication

7. Final Project's Topics (include but not limit)

Cipher Game(local encryption)

- AES-GCM Application
- AES+（DIY）

Cipher Game Plus

- WebCrypto API with KMS
- Communication with PKI and KMS

Cipher Game Pro

- Simulation CSE
- File System's Authority Management with PKI

Cipher Game Pro Max

- Simulation CSE（included multi-nodes \ WebCrypto API \ >3 users \ KMS）