Lucid

Lucid Key Management Service

Technical Specifications

James Judd, Sr. Director, Engineering
Nathan Cooper, Security Architect

Lucid helps teams see and build the future from idea to reality. The power, simplicity, affordability, and security of the Lucid Visual Collaboration Suite have driven its adoption by millions of individuals and teams. The following paper introduces our Lucid Key Management Service (KMS), which allows customers to control their own encryption keys for an additional layer of security and the technical specifications related to this feature.

Lucid Software, Inc.
10355 South Jordan Gateway
Suite 300
South Jordan, UT 84095 USA

www.lucid.co
sales@lucidchart.com
1-650-733-6172

v220623-1130

Overview

Lucid Key Management Service (KMS) provides additional security and control to Lucid's already secure platform, allowing customers to manage the encryption keys securing their data. Lucid KMS offers the following features:

- Controlled data access via customer-managed encryption keys
- Logs related to customer Key Encryption Key access for easier auditing
- Unique encryption keys for every account

When implemented as Lucid recommends, Lucid KMS provides industry-leading data protection without impacting end-user performance. Envelope encryption offers an added layer of security, and audit logs provide additional control over the protection of customer data.

How Lucid KMS works

Lucid KMS utilizes two kinds of keys: Key Encryption Keys (KEK) and Data Encryption Keys (DEK). Data Encryption Keys are used to encrypt and decrypt customer data. Key Encryption Keys are used to encrypt and decrypt the Data Encryption Keys. Every Lucid account with KMS enabled has a KEK and at least one DEK. Lucid KMS is an extra layer of security in addition to Lucid's standard secure encryption. Lucid's standard secure encryption is applied to all customer data regardless of account options. Our KMS applies an additional layer of envelope encryption to document data when it's at rest. Data in transit continues to be protected with our standard encryption.

Lucid does not have access to the customer's KEK. This key is generated and stored securely within AWS's Key Management Service (AWS KMS). The Key Encryption Key cannot be exported or otherwise retrieved.

High-level process for data at rest

The customer's document is initially encrypted using a DEK. The DEK is then sent to AWS KMS to be encrypted by the customer's KEK. The now-Encrypted Data Encryption Key (EDEK) and the encrypted document are stored in Lucid's database. Lucid classifies certain parts of our infrastructure, e.g., Elasticsearch indexes, as data in transit. This data follows our standard encryption process. To decrypt data at rest, e.g., an encrypted document, the process is followed in reverse.

Document encrypted with Lucid key

Lucid encrypts all user documents as a first layer of security.

Lucid key encrypted with customer key

Add an extra layer of security with no impact on usability or speed.

Customer key stored in KMS

Lucid can never see or access your key encryption key—you're always in complete control of your documents.

Audit log updated

An immutable audit log tracks and preserves each and every use of your encryption key.

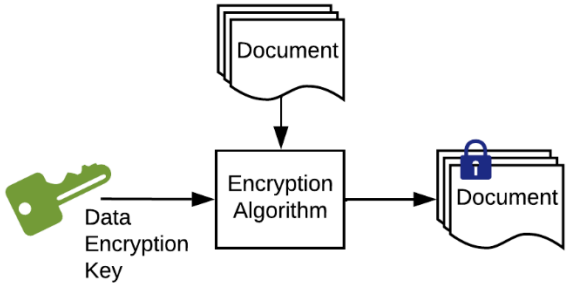
Detailed encryption process

Lucid uses the following process to encrypt customer documents:

1. The customer creates a new document, or Lucid KMS is enabled for the customer's account.

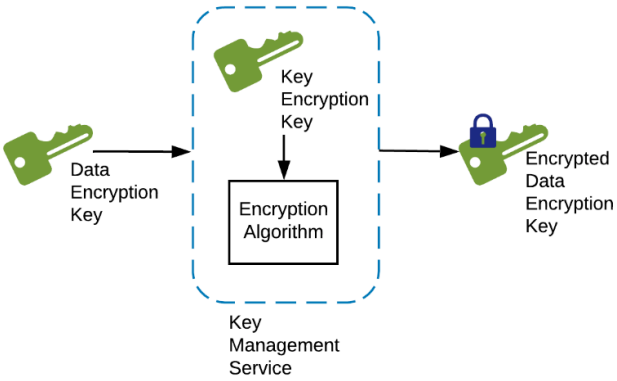
---

2. A DEK is created if a valid DEK does not already exist for the customer, and the customer's document is encrypted with that DEK.



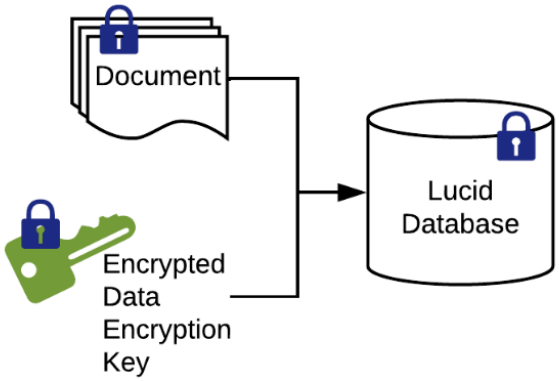
---

3. Lucid sends the DEK to AWS KMS or CloudHSM to be encrypted with the account's KEK.



---

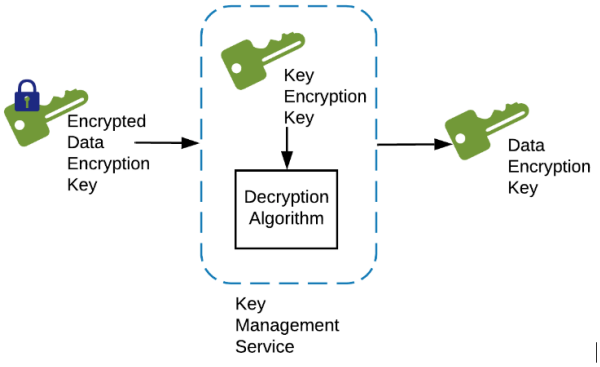
4. The encrypted DEK is then stored alongside the encrypted data in Lucid's database (persisted on an encrypted volume).



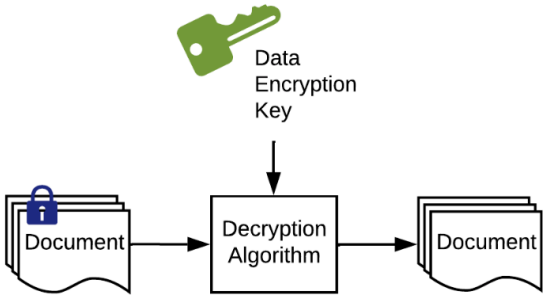
Detailed decryption process

Data is decrypted in a similar manner.

1. The encrypted DEK associated with a document is retrieved from Lucid's database and is sent to AWS KMS or CloudHSM to be decrypted using the account's KEK.

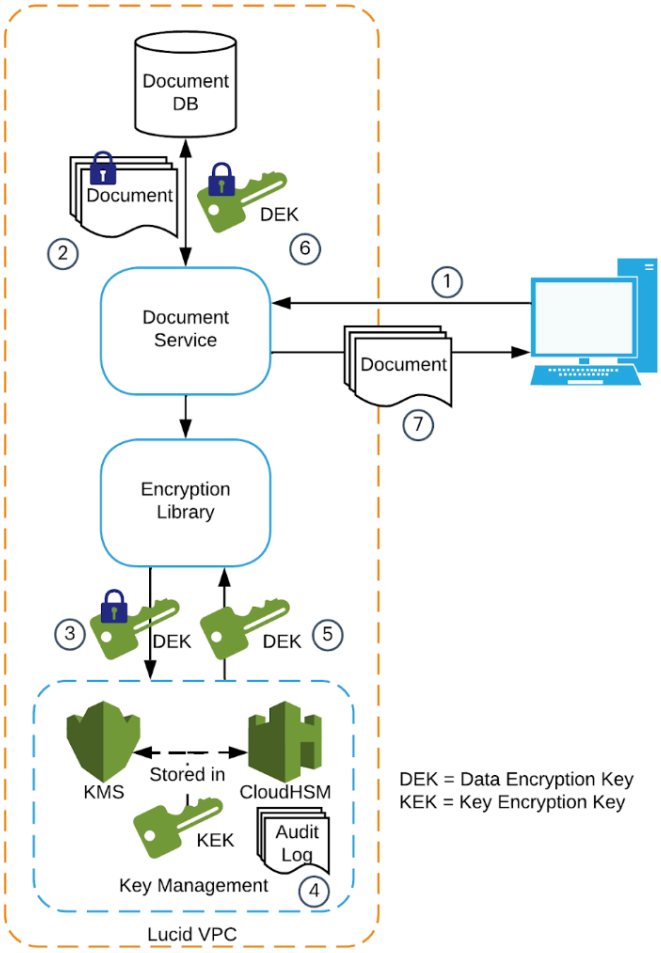


2. The encrypted document is decrypted using the decrypted DEK.



KMS example

Lucid uses the following process to retrieve a requested customer document:



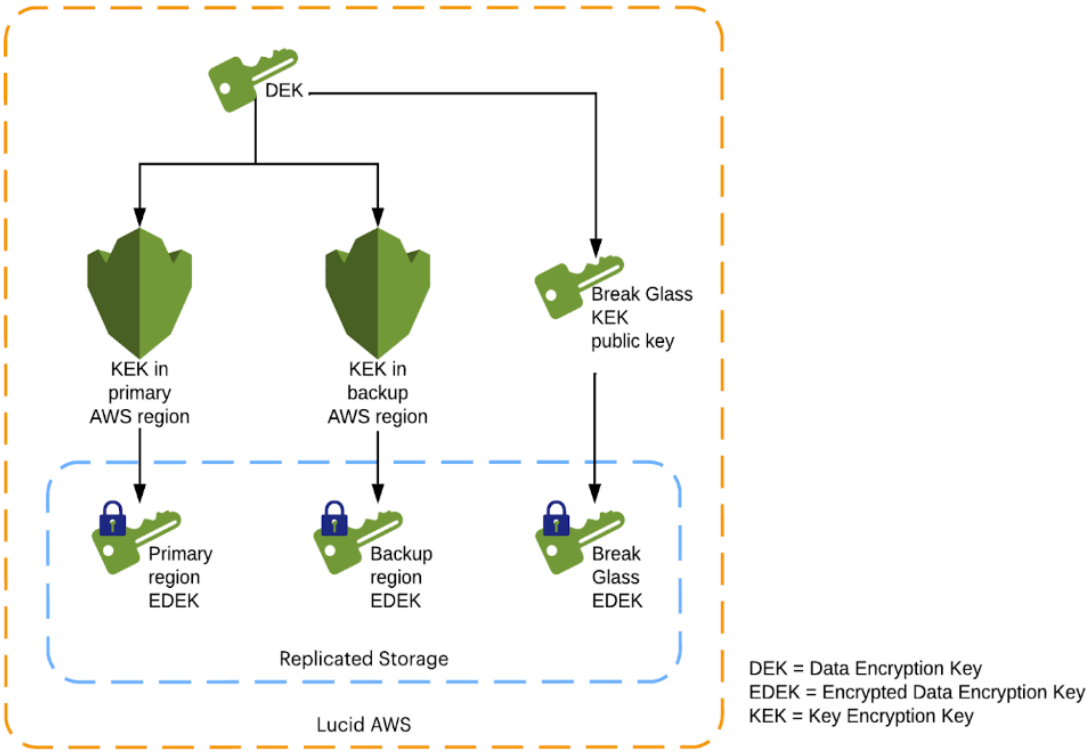
1. The customer requests their document.
2. The encrypted document and encrypted Data Encryption Key are retrieved from the database by the Lucid Document Service.
3. The encrypted Data Encryption Key is sent to AWS KMS or CloudHSM to be decrypted using the customer's Key Encryption Key.
4. This request generates an entry in an immutable audit log.
5. The decrypted Data Encryption Key is sent back to the Document Service.
6. The Data Encryption Key is used to decrypt the document.
7. The decrypted document is returned to the customer.

Break Glass Key and Disaster Recovery

Lucid's KMS offering includes a Break Glass Key (BGK), which serves as an additional Key Encryption Key for all Data Encryption Keys. The BGK utilizes asymmetric encryption, with Lucid's document services holding the public portion of the key. This public key separately encrypts the Data Encryption Keys used to encrypt the customer's data in addition to the customer's regular Key Encryption Key. The private portion of the BGK is encrypted, stored securely, and shared with a group of Lucid executives. The information required to decrypt the private portion of the key is securely stored separately from the encrypted key and shared with a different group of Lucid executives. To access the private portion of the BGK, at least two Lucid executives are required - one with access to the encrypted private portion of the key and another with access to information required to decrypt it.

The Break Glass Key supports the disaster recovery capabilities of the system, ensuring a customer can continue to access their data in the event of a key-related disaster.

This system can be seen in the following diagram:



Lucid KMS features

The following features are provided as part of Lucid Key Management Service.

Envelope encryption

Envelope encryption is the process of using encrypted keys to protect your sensitive data. This is an industry best practice and envelope encryption is supported by major cloud providers including Box and Salesforce.

Key generation

When KMS is enabled, a customer-specific Key Encryption Key is generated by Amazon using AWS KMS. Lucid then generates Data Encryption Keys, encrypts sensitive customer data using those DEKs, encrypts the DEKs (turning them into EDEKs), and stores the encrypted DEK (EDEK) on encrypted volumes.

Key rotation

KMS enables the customer to rotate their KEK once every 24 hours or if there is evidence that Lucid's security has been compromised. Key rotation can be executed manually as well. When the KEK is rotated, a new KEK is generated. Customer DEKs are decrypted using the current KEK and then re-encrypted using the new KEK. The current KEK is then deactivated for future encryption operations once all data keys have been encrypted using the new KEK.

Key revocation

After KEKs are rotated, keys no longer in use are deactivated but not deleted. Customer Key Encryption Keys remain in AWS KMS. These deactivated keys are used in the event that backups need to be restored. KEKs can be purged upon request.

Audit logs

All actions performed using a customer's DEKs and KEKs are tracked and logged in an immutable audit log.

About Lucid

Lucid offers a leading visual collaboration suite that helps teams see and build the future from idea to reality. With its products—Lucidchart, Lucidspark, and Lucidscale—teams can align around a shared vision, clarify complexity, and collaborate visually, no matter where they're located. Top businesses use Lucid's products all around the world, including customers such as Google, GE, NBC Universal, and T-Mobile. Lucid's partners include industry leaders such as Google, Atlassian, Amazon Web Services, Salesforce, and Microsoft. Since the company's founding, it has received numerous awards for its products, business, and workplace culture. For more information, visit Lucid.co.