Lucid

Lucid Key Management Service

Technical Specifications

James Judd, Sr. Manager, Engineering
Nathan Cooper, Senior Security Engineer

Lucid is the only visual collaboration suite that helps teams see and build the future from idea to reality. Its products, Lucidchart and Lucidspark, provide users with an end-to-end experience that helps teams truly see and build the future, by enabling collaboration and clear communication. The power, simplicity, affordability, and security of Lucid have driven its adoption by millions of individuals and teams from numerous businesses and educational institutions.

The following paper introduces Lucid Key Management Service (KMS), which allows businesses 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

v210303-1812

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. KMS provides the customer the following features:

- Control over access to customer data, via control over access to encryption keys
- Easier auditing via logs related to master key access
- Unique encryption keys per account

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

How Lucid KMS works

Lucid KMS supports two kinds of keys: *master keys* and *data keys*. Data keys, also known as *data encryption keys (DEK)*, are used to encrypt and decrypt customer data. Master keys, also known as *key encryption keys (KEK)*, are used to encrypt and decrypt the data keys. Every Lucid account with KMS enabled has a master key and at least one data key.

Lucid does not have access to the customer's master key. It is generated and stored securely in AWS Key Management Service (AWS KMS) or a managed hardware security module on AWS Cloud (Amazon CloudHSM). The master key cannot be exported or otherwise retrieved.

High-level process

The customer's document is initially encrypted using a data key. The data key is then sent to AWS KMS or a CloudHSM to be encrypted by the customer's master key. The now-encrypted data key and the encrypted document are stored in Lucid's database and the customer retains their own master key.

To decrypt an encrypted document, the process is followed in reverse.

Document encrypted with Lucid key

Lucidchart 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 or HSM

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

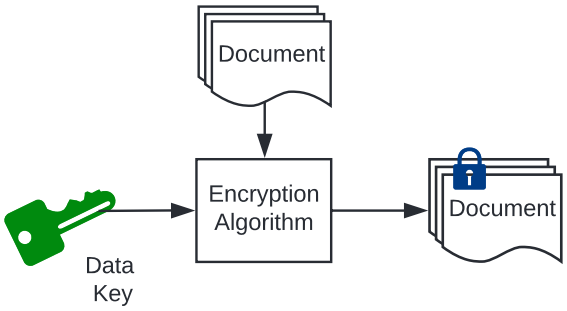
Audit log updated

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

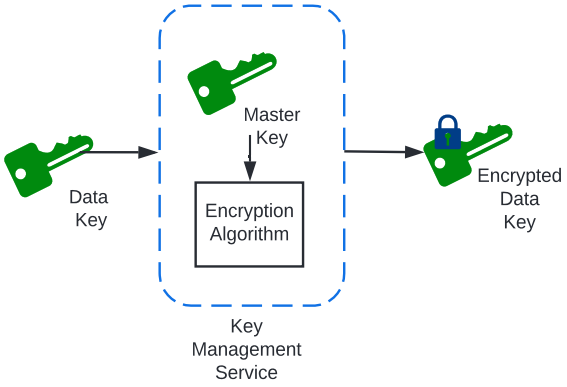
Detailed process

Lucid undergoes the following process to encrypt customer documents.

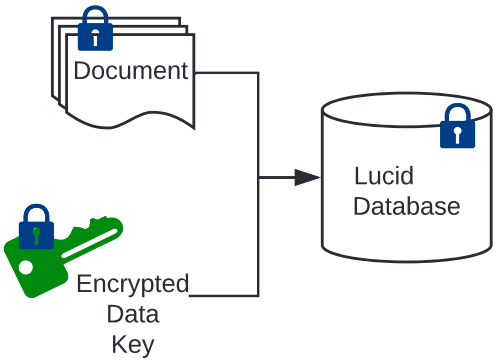
1. A data key is created, and the customer's document is encrypted with that data key.



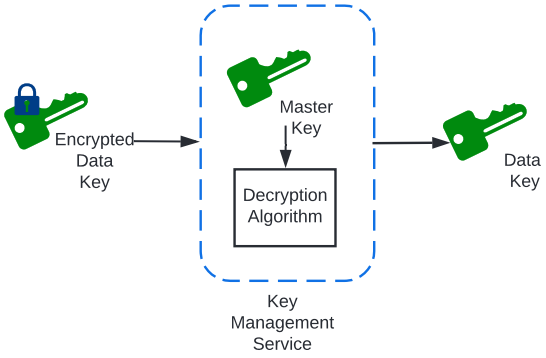
2. Lucid sends the data key to AWS KMS or a CloudHSM to be encrypted with the account's master key.



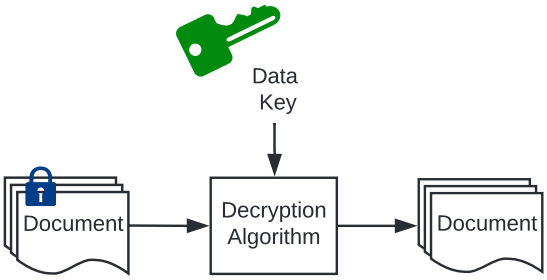
3. Lucid then stores the encrypted data key alongside the encrypted data in our database (persisted on an encrypted volume).



1. Data is decrypted in a similar manner.
2. First, the encrypted data key is sent to AWS KMS or a CloudHSM to be decrypted using the master key.

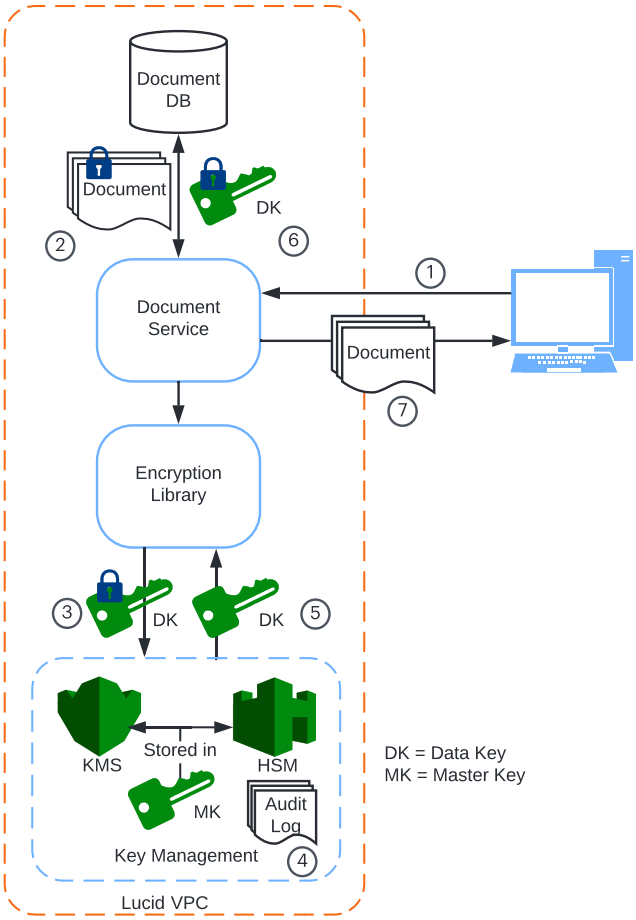


3. The encrypted document is decrypted using the decrypted data key.



KMS example

Lucid undergoes the following process to retrieve a requested customer document.



1. The customer requests their document.
2. The encrypted document and encrypted data key (DK) are retrieved from the database by the Lucidchart Document Service.
3. The encrypted data key is sent to AWS KMS or a CloudHSM to be decrypted using the customer's master key (MK).
4. This request generates an entry in an immutable audit log.
5. The decrypted data key is sent back to the Document Service.
6. The decrypted data key is used to decrypt the document.
7. The decrypted document is returned to the customer.

Lucid KMS features

Read about the features provided as part of Lucid Key Management Service.

Envelope encryption

Envelope encryption is an industry best practice and is supported by major cloud providers including Box and Salesforce. Documentation on envelope encryption can be found at Amazon AWS, Google Cloud Platform, and Microsoft Azure.

Key generation

When KMS is enabled, a master key is generated on behalf of the customer by Amazon using AWS KMS or a CloudHSM. Lucid then generates data keys, encrypts sensitive customer data using those data keys, encrypts the data keys, and stores the encrypted data keys on encrypted volumes.

Key rotation

KMS enables the customer to rotate their master key once every 24 hours or if there is evidence that Lucidchart's security has been compromised. Key rotation can occur manually.
When the master key is rotated, a new master key is generated. All of the customer's data keys are decrypted using the current master key and then re-encrypted using the new master key. The current master key is deactivated once all data keys have been encrypted using the new master key.

Key revocation

After master keys are rotated, keys no longer in use are deactivated, but not deleted. Master keys remain in AWS KMS or an Amazon CloudHSM. These deactivated keys are used in the event that backups need to be restored. Master keys can be purged upon request.

Audit logs

All actions performed using a customer's data keys and master keys are tracked and logged in an immutable audit log.

About Lucid

Lucid is the only visual collaboration suite that helps teams see and build the future from idea to reality. Its products, Lucidchart and Lucidspark, provide users with an end-to-end experience that helps teams truly see and build the future, by enabling collaboration and clear communication. Lucidspark is a virtual whiteboard application for freeform ideation, group brainstorming and real-time collaboration across teams. Lucidchart is an intelligent diagramming application for understanding the people, processes and systems that drive business forward. Lucid products are utilized in over 180 countries by more than 30 million users, including customers like Google, GE, NBC Universal and Johnson & Johnson and ninety-nine percent of the Fortune 500. Lucid's partners include industry leaders such as Google, Atlassian, Amazon Web Services, Salesforce and Microsoft. Since the Utah-based company's founding in 2010, it has received numerous awards for its product, business and workplace culture. For more information, visit lucid.co.