DataRow Key Management Service

Technical Specifications

D. Can Abacigil, CTO

6 FEBRUARY 2019

DataRow, provided by TeamSQL, Inc. is a database client for Amazon Redshift, to help users save time and money while managing and developing their data.

The following paper introduces DataRow 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

TeamSQL, Inc.
WeWork Mid-Market 995
San Francisco CA 94103
United States
Email: sales@datarow.com
Website: www.datarow.com

Overview

DataRow Key Management Service (KMS) provides additional security and control to DataRow'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, DataRow 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 DataRow KMS works

DataRow 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 DataRow account (all accounts are KMS enabled by default) has a master key and at least one data key. DataRow does not have access to the customer's master key. It is generated and stored securely in AWS Key Management Service (AWS KMS). The master key cannot be exported or otherwise retrieved.

High-Level Process

A customer master key is generated by AWS KMS when a user is registered. This CMK is unique and stored in AWS KMS.

Whenever a customer data will be stored in DataRow servers, DataRow generates a unique data key for each entity in DataRow databases.

The data key is then sent to AWS KMS to be encrypted by the customer's master key. The now-encrypted data key and the encrypted customer data are stored in DataRow's database.

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

1. Customer data encrypted with DataRow key

First layer of security, all customer data is encrypted.

2. DataRow key encrypted with customer key

Envelope encryption is an industry best practice and is supported by major cloud providers.

3. Customer key stored in AWS KMS

DataRow can never see or access your encryption keys.

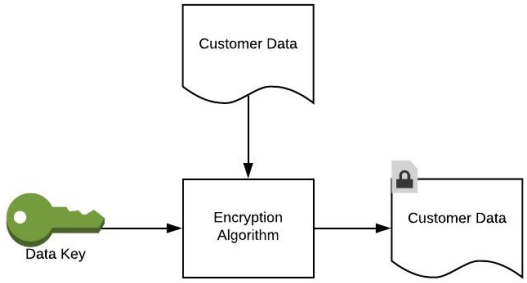
4. Customer key stored in AWS KMS

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

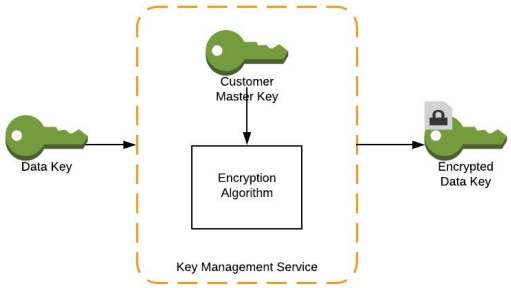
Detailed Process

DataRow undergoes the following process to encrypt customer data.

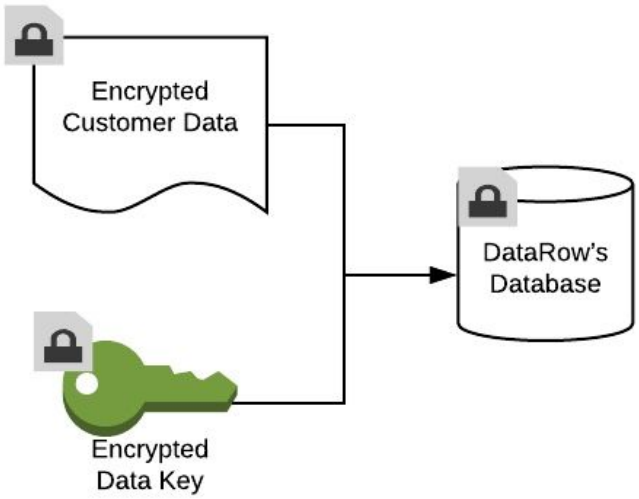
1. A data key is generated using DataRow's master key and the customer data is encrypted with that data key.



2. DataRow sends the data key to AWS KMS to be encrypted with the customer's master key.



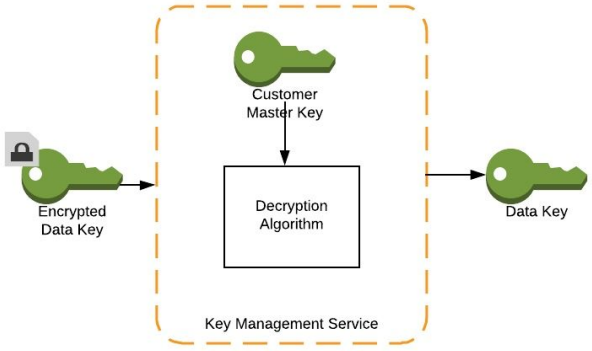
3. DataRow stores the encrypted data key alongside the encrypted data in DataRow's database (persisted on an encrypted volume).



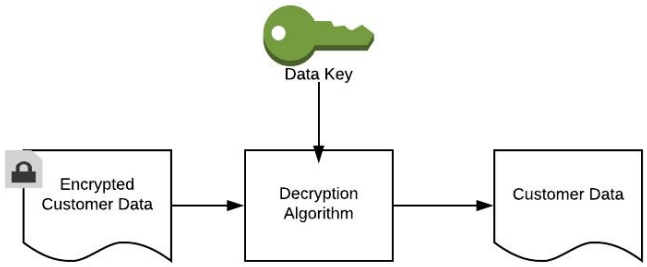
Detailed Process (continues)

Data is decrypted in a similar way.

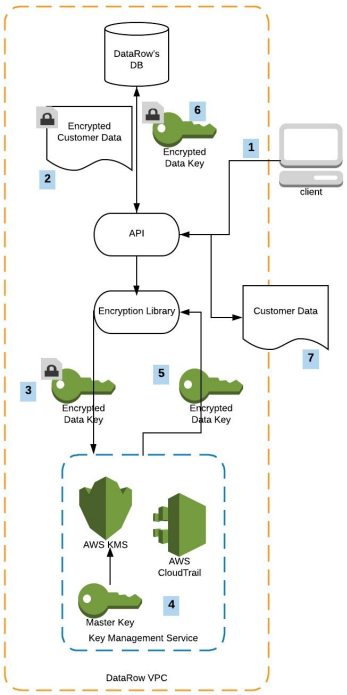
1. The encrypted data key is sent to AWS KMS to decrypted using customer key.



2. The encrypted data is decrypted using the decrypted data key.



KMS Example



1. The customer requests their data.
2. The encrypted document and encrypted data key are retrieved from the database by the DataRow API.
3. The encrypted data key is sent to AWS KMS to be decrypted using the customer's master key.
4. This request generates an entry in an immutable audit log.
5. The decrypted data key is sent back to the DataRow API.
6. The decrypted data key is used to decrypt the customer data.
7. The decrypted customer data is returned to the customer.

DataRow KMS Features

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. DataRow 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 DataRow'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. This is a manual process can be done by DataRow.

Key revocation
After master keys are rotated, keys no longer in use are deactivated, but not deleted. Master keys remain in AWS KMS.
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.