**Customer master key (CMK)**

Encryption at rest protects your DynamoDB tables under an AWS KMS customer master key (CMK).

DynamoDB supports only [symmetric CMKs](https://docs.aws.amazon.com/kms/latest/developerguide/symm-asymm-concepts.html#symmetric-cmks). You cannot use an [asymmetric CMK](https://docs.aws.amazon.com/kms/latest/developerguide/symm-asymm-concepts.html#asymmetric-cmks) to encrypt your DynamoDB tables.

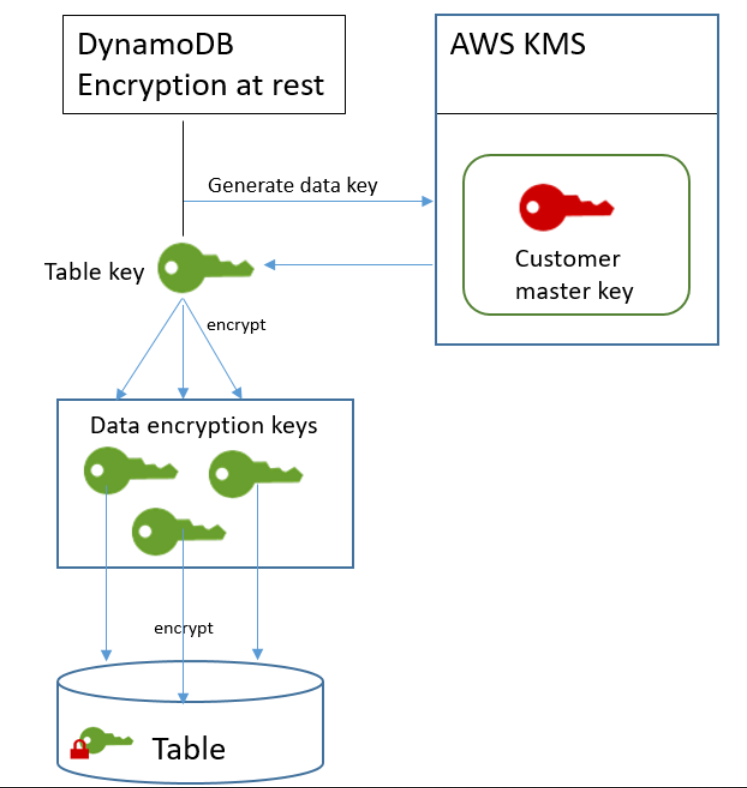
You can choose your CMK in the DynamoDB console or by using DynamoDB API. When you select a CMK for a table, the local and global secondary indexes, streams, and backups are encrypted with the same CMK. However, you cannot use a customer managed CMK to encrypt DynamoDB global table replicas. To encrypt replicas, use an AWS owned CMK or an AWS managed CMK.

Use a customer managed CMK to get the following features:

* You create and manage the CMK, including setting the [key policies](https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html), [IAM policies](https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies.html) and [grants](https://docs.aws.amazon.com/kms/latest/developerguide/grants.html) to control access to the CMK. You can [enable and disable](https://docs.aws.amazon.com/kms/latest/developerguide/enabling-keys.html) the CMK, enable and disable [automatic key rotation](https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html), and [delete the CMK](https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html) when it is no longer in use.
* You can use a customer managed CMK with [imported key material](https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys.html) or a customer managed CMK in a [custom key store](https://docs.aws.amazon.com/kms/latest/developerguide/custom-key-store-overview.html) that you own and manage.
* You can audit the encryption and decryption of your DynamoDB table by examining the DynamoDB API calls to AWS KMS in [AWS CloudTrail logs](https://docs.aws.amazon.com/kms/latest/developerguide/services-dynamodb.html#dynamodb-cmk-trail).

**Table keys**

DynamoDB uses the CMK for the table to generate and encrypt a unique [data key](https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#data-keys) for the table, known as the *table key*. The table key persists for the lifetime of the encrypted table.



**Table key caching**

To avoid calling AWS KMS for every DynamoDB operation, DynamoDB caches the plaintext table keys for each connection in memory.