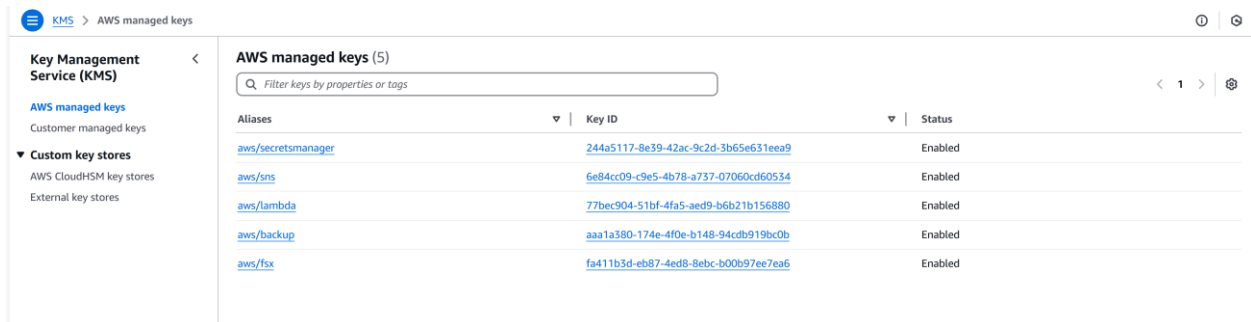


## NETSEC-002 - Define data encryption policy for data at rest and in transit

The services de Directory are implement using certificates issued by the Certificate Manager service are associated. The Organization using AWS manager Keys.

**Cryptographic keys are managed securely**

**Encryption keys are controlled by AWS**



The screenshot displays the AWS KMS console interface. On the left, a navigation pane shows 'Key Management Service (KMS)' with options for 'AWS managed keys' and 'Custom key stores'. The main area is titled 'AWS managed keys (5)' and contains a table of active keys. The table has three columns: 'Aliases', 'Key ID', and 'Status'. Five keys are listed, all with 'Enabled' status. The keys are associated with various AWS services: secretsmanager, sns, lambda, backup, and fsx.

Aliases	Key ID	Status
<a href="#">aws/secretsmanager</a>	244a5117-8e39-42ac-9c2d-3b65e631eea9	Enabled
<a href="#">aws/sns</a>	6e84cc09-c9e5-4b78-a737-07060cd60534	Enabled
<a href="#">aws/lambda</a>	77bec904-51bf-4fa5-aed9-b6b21b156880	Enabled
<a href="#">aws/backup</a>	aaa1a580-174e-4f0e-b148-94cdb919bc0b	Enabled
<a href="#">aws/fsx</a>	fa411b3d-eb87-4ed8-8ebc-b00b97ee7ea6	Enabled