

**Qualcomm Car-to-Cloud Platform**

**KMS INTERFACE DOCUMENT**

**Version No.2.0**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Prepared By / Last Updated By** | **Reviewed By** | **Approved By** |
| **Name** | Anusree B | Sudheer | Sudheer |
| **Role** | PAT | Sr Manager | Sr Manager |
| **Signature** |  |  |  |
| **Date** | 18/05/2021 | 11/06/2021 | 11/06/2021 |

May 18, 2021

Cognizant

Table of Contents

[1. KMS INTERFACE 2](#_Toc74563511)

[2. INTERFACE APPLICATION 2](#_Toc74563512)

[2.1 c2c\_base\_key\_management\_service\_intf 3](#_Toc74563513)

[2.2 c2c\_base\_kms\_aws\_impl 4](#_Toc74563514)

# KMS INTERFACE

An interface contains variables and signatures of function. Other classes that implement the interface can implement these signatures. This functionality improves the flexibility and stability of programs and applications.

A significant way to utilize this functionality is by separating the interface and its implementation through converting the interface as jar and adding it to its implementation as a dependency. This separation of interface enables the possibility of having multiple implementations for the same interface.

**FEATURES**

* An interface project that outlines the signatures of basic functionalities.
* An implementation project that implements the signatures in the interface project.
* A base class whose main purpose is to call the implemented methods and determine the flow of the application.
* An ability to change the implementation by changing the jar file in the application without changing or affecting the flow of the base program.

The idea is to use this concept to provide a common Cloud Agnostic Method.

# INTERFACE APPLICATION

Consider a sample KMS application - that is meant to encrypt and decrypt a message using a key via cloud services. For this application, AWS Key Management Service (KMS) has been used.

The project can be divided into two projects –

* **c2c\_base\_key\_management\_service\_intf,** which contains the interfaces containing signatures of functions related to encrypt, decrypt and reconnect.
* **c2c\_base\_kms\_aws\_Impl**, which contains the implementation of the function signatures in c2c\_base\_key\_management\_service\_intf. The implementations will be responsible for encryption and decryption of messages using AWS KMS and client reconnection.

## c2c\_base\_key\_management\_service\_intf

c2c\_base\_key\_management\_service\_intf is the KMS interface project that contains the signatures of encrypt, decrypt and reconnect functions. It contains the following classes:

* IC2CKeyManagement

IC2CKeyManagement is the interface that contains the following function signatures:

* + public String encrypt(String payload, String keyId, String keyVersionId, String keyRingId, boolean isSymmetric) throws KeyManagementApplicationException

Function signature for for encrypting the payload using the keyId, keyVersionId, keyRingId based on the value of isSymmetric. The value of isSymmetric will be true for symmetric key encryption and false for asymmetric key encryption. For AWS, keyVersionId and keyRingId will be null.

* + public String decrypt(String encryptedPayload, String keyId, String keyVersionId, String keyRingId, boolean isSymmetric) throws KeyManagementApplicationException

Function signature for decrypting the encryptedPayload using the keyId, keyVersionId, keyRingId based on the value of isSymmetric. For AWS, keyVersionId and keyRingId will be null.

* + public boolean reconnect()

Function signature for reconnection of the client for any connection failure scenarios.

* C2CKeyManagementConnectionConfig

C2CKeyManagementConnectionConfig is the configuration class that contains the AWS KMS connection variables and their getters and setters. It has a Builder class which has a build() method to create the C2CKeyManagementConnectionConfig object.

* Custom exception classes in c2c\_base\_key\_management\_service\_intf are:
* KeyManagementApplicationException

Custom exception thrown when a generic KMS exception occurs in encrypt or decrypt methods.

## c2c\_base\_kms\_aws\_impl

c2c\_base\_kms\_aws\_impl is the KMS implementation project that contains the implementation for each method signature in the interface. It contains following class:

* C2CKeyManagementImpl

This class contains:

* + A single argument constructor that initializes the connection variables using the C2CKeyManagementConnectionConfig object passed by the caller project. The constructor also calls getConnection() method that establishes the connection to client.
  + Method body for encrypt, decrypt and reconnect methods.
  + A private method getStringFromByteBuffer() to convert ByteBuffer to String during decryption.
  + A private getConnection() method that builds the AWS KMS client.
* KMSConstants

This is an abstract class that defines the constants used in C2CKeyManagementImpl.

* KMSOperationErrors

This is an enum class that contains enums used in exception messages.

* This project uses the jar of

c2c\_base\_key\_management\_service\_intf project.