Decryption logic at our end: - (Reference)

Please download the JOSE module node js lib and refer the same. Below one is IBM Specific.

var jose = require('jose');

var privateKey = 'indus-privatekey'; //referring private key

if (privateKey != null) {

context.request.body.readAsJSON(function (error, json) {

if (error) {

context.reject('CustomError', 'Request not in JSON');

} else {

var data = json.data

var bit = json.bit

var jweobj = jose.parse(json.key);

jweobj.setKey(privateKey);

jose.createJWEDecrypter(jweobj).decrypt(function (error, symmetricKey) { //decrypt the symmetric key using private key

if (error) {

context.reject('CustomError', 'JWE Decryption Failed with Certificate');

} else {

var aesHexKey

if (bit == 0){aesHexKey = symmetricKey}

if (bit == 1){aesHexKey = symmetricKey.toString('hex');}

context.set("mySymmetricKey", aesHexKey);

var jweobj = jose.parse(data);

jweobj.setKey('hex:' + aesHexKey);

jose.createJWEDecrypter(jweobj).decrypt(function (error, plaintext) { //decrypt the payload

if (error) {

context.reject('CustomError', 'JWE Decryption Failed with AES Key');

} else {

var decryptedJson = json

decryptedJson = JSON.parse(plaintext.toString());

context.message.body.write(decryptedJson);

}

});

}

});

}

});

}

Encryption Logic at our end: -

var jose = require('jose');

var jweHdr = jose.createJWEHeader('A256GCM'); //supported algorithm for encryption

var mySymmetricKey = context.get('mySymmetricKey');

jweHdr.setProtected('alg', 'A256KW');

jweHdr.setKey('hex:' + mySymmetricKey);

context.message.body.readAsJSON(function (error, json) {

if (error) {

context.reject('CustomError', 'Response not in JSON');

} else{

var \_my\_json\_string = JSON.stringify(json);

let \_my\_json\_buffer = new Buffer(\_my\_json\_string);

jose.createJWEEncrypter(jweHdr).update(\_my\_json\_buffer).encrypt('compact', function (error, jweObj) {

if (error) {

context.reject('CustomError', 'JWE Encryption Failed');

} else {

context.message.body.write({"data": jweObj});

}

}

);

}

}

);

IBM Knowledge Centre reference: -

https://www.ibm.com/docs/en/datapower-gateway/10.0.1?topic=apis-jose-module