

|  |
| --- |
| 加密規則(本加密步驟主要使用AES加密碼來產生最終產物)( CipherMode=CBC) |
| 1.不用產生公鑰 直接用私鑰解即可 |
| 2."Eki1qaz@WSX123" 使用SHA256產生一組hash code(需去除"-") |
| 3.hashCode 取0-16(Substring(0, 16))字串->ASCII encode-> MD5 轉換->byte[]來當加密的key(AES) |
| 4.hashCode 從8的位置之後取24碼(Substring(8, 24)) ->ASCII encode ->MD5->轉換成byte[]來當加密的hashIV(AES) |
| 5.將data轉換成base64 byte[] |
| 6.使用設定好的(Key,IV) AES來解密 |

付款完成頁面的header中 帶有使用者付款的資料

Key:data

測試用:

0J4FyjrzuRA565jMhlTbF5xVz38Gj+l7XEl3nfXe2OiwIDGKfI2gEPle0cXdZq+3A6xVUV0L5JgM6fWVGsirgQ==

結果:

{

"OrderSerial": "CPS16523435283889835",

"Msg": "授權成功"

}