|  |  |  |  |
| --- | --- | --- | --- |
| member forget password | 會員忘記密碼的修改api |  | **\*紅色框為必填** |
| API url:http://cpsapi.eki.com.tw/api/member/ForgetPwd | | | |
| **Method** | **POST** |  |  |
| **Header** | |  |  |
| **secret** | | 隨機碼(8碼) |  |
| **token** | | Eki+secret+!qaz2WSX#edc 使用SHA256編碼完去除"-" 都大寫 | |
| **Body** | |  |  |
| **Content-Type** | | application/json |  |
| **key** | **string** | **public key length>5** |  |
| **content** | string | member pwd information json object text encode |  |
| PwdInfo |  |  |  |
| phone | string | member phone number | |
| pwd | string | member pwd |  |
| 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.隨機生成至少5碼的公鑰(publicKey) | | | |
| 2.publicKey+"!qaz2WSX#edc" 使用SHA1產生一組hash code(需去除"-") | | | |
| 3.hashCode 取0-16(Substring(0, 16))字串使用ASCII encode過在 MD5 轉換成byte[]來當加密的key(AES) | | | |
| 4.hashCode 從字串長度8的位置之後取8碼(Substring(8, 8)) 使用ASCII encod 過在使用MD5轉換成byte[]來當加密的hashIV(AES) | | | |
| 5.將PwdInfo轉換成json string後使用UTF8 encode 生成byte[]當作加密的文本 | | | |
| 6.轉換成base64 string | | | |

Request Sample:

{

"key":publickey,

"content":content

}

Response:

{

"success": true,

"message": "success",

"errorCode": "E000"

}

更新日誌:

2022/06/15:

init