中華電信

MQTT認證機制

V2.02

MQTT 雙向認證加密協定

(1) 終端設端 MqTT 的訂閱與發佈客製化 Adaptor (iot-encmqtt)並申請 port 3883

Hostname	iot.cht.com.tw		Port	3883
Username	kms	Password	Project Key or Device Key	

Payload: ICCID+FAN_ID+Random+HMAC

KMS Publish Data [flag 0 加密內容]: (rawdata/command/ack)payload: Base64(procId[4]+flag[1]+eData+CRC[4])

byte[]組成, eData 為 enc(Rawdata JSON String)

procId 為 int 數值

flag 為發佈類型: 0 表示加密內容; 1 表示認證加密內容

eData 為加密資料

Method	Topic	
Subscribe	/v1/kms/device/{deviceId}/rand	訂閱取得認證亂數 Message: 未加密字串
Publish	/v1/kms/device/{deviceId}/auth	發送認證比對資訊 Payload: Base64 字串
Publish	/v1/kms/device/{deviceId}/auth/byte	發送認證比對資訊 Payload: Byte Array
Subscribe	/v1/kms/device/{deviceId}/auth/{rand}	訂閱認證比對結果 Message: 未加密字串

Subscribe	/v1/kms/device/{deviceId}/sensor/{sensorId}/rawdata	訂閱感測數據 Message: Base64 字串
Subscribe	/v1/kms/device/{deviceId}/sensor/{sensorId}/rawdata/byte	訂閱感測數據 Message: Byte Array
public	/v1/kms/device/{deviceId}/rawdata	發佈加密感測數據 Payload: Base64 字串
public	/v1/kms/device/{deviceId}/rawdata/byte	發佈加密感測數據 Payload: Byte Array
public	/v1/kms/device/{deviceId}/rawdata	發佈加密感測數據 Payload: Base64 字串

(2) 終端設端 MqTT 的連線設定並申請 port 1883，DeviceKey 經由雙向認證共同金鑰加密後，以 Base64 編碼字串格式

◆ 認證訊息(Payload)

Publish /v1/kms/device/{deivceId}/auth

payload: Base64(ICCID+FAN_ID+Random+HMAC)

將 Byte array 組合起來後以 Base64 編碼為字串格式

Hostname	iot.cht.com.tw		Port	1883
Username	ekms	Password	Base64(enc(DeviceKey))	

名稱	位置	說明	格式	描述
ICCID	[0-31]	ICCID	Byte Array [32 bytes]	ICCID，共 32 bytes
FAN_ID	[32-47]	FAN_ID	Byte Array [16 bytes]	FAN_ID，共 16 bytes
Rand	[48-63]	Random data	Byte Array [16 bytes]	Random，共 16 bytes
HMAC	[64-83]	HMAC	Byte Array [20 bytes]	HMAC 值，共 20 bytes

◆ 上傳加密訊息(Payload)

Publish /v1/kms/device/{deivceId}/rawdata

payload: Base64(procId[4]+flag[1]+CRC[4]+eData)

(eData 為 enc(Rawdata/Command/Ack JSON 字串))

procId 為上傳感測數據編號，配合訂閱數據加解密處理狀態通知，此編號用來識別處理狀態

flag 為識別 payload 為加密內容還是認證加密內容格式 (注意: 0,1 為字串格式)

checksum 為計算 eData 的循環冗餘校驗結果

eData 將上傳感測數據 JSON 字串透過雙向認證共同金鑰加密

將 Byte array 組合起來後以 Base64 編碼為字串格式

名稱	位置	說明	格式	描述
procId	[0-3]	發送編號	int [4 bytes]	使用 Little Endian 位元組順序
flag	[4]	發佈類型	String [1 byte]	"0" (0x30) 加密內容 "1" (0x31) 認證加密內容 ※ ASCII byte
checksum	[5-8]	循環冗餘校驗	long [4 bytes]	計算 eData 的循環冗餘校驗(CRC32)
eData	[9-…]	加密資料	Byte Array	加密資料

◆ 上傳加密及認證訊息(Payload)

Publish /v1/kms/device/{deivceId}/rawdata
payload: Base64(procId[4]+flag[1]+CRC[4]+eData)
(eData 為 enc(Rawdata/Command/Ack JSON 字串))

名稱	位置	說明	格式	描述
procId	[0-3]	發送編號	int [4 bytes]	使用 Little Endian 位元組順序

flag	[4]	發佈類型	String [1 byte]	"0" (0x30) 加密內容 "1" (0x31) 認證加密內容 ※ ASCII byte
ICCID	[5-36]	ICCID	Byte Array [32 bytes]	ICCID，共 32 bytes
FAN_ID	[37-52]	FAN_ID	Byte Array [16 bytes]	FAN_ID，共 16 bytes
Rand	[53-68]	Random data	Byte Array [16 bytes]	Random，共 16 bytes
HMAC	[69-88]	HMAC	Byte Array [20 bytes]	HMAC 值，共 20 bytes
Checksum	[89-92]	CRC	long [4 bytes]	計算 eData 的循環冗餘校驗(CRC32)
eData	[92-…]	加密資料	Byte Array	加密資料

◆ 認證(auth)回傳結果

回傳格式: (字串)狀態碼,狀態描述(錯誤描述)

回傳資訊(String)	資訊說明	備註
0	OK	
401,Incorrect random	亂數資料不正確	

402,ICCID error	ICCID 錯誤	
403,FAN ID error	FAN ID 錯誤	
404,HMAC error	HMAC 錯誤	
405,Incorrect checksum	Checksum 錯誤	
440,KMS Server error	KMS Server 錯誤	
441,KMS data error	KMS 回傳資料格式錯誤	回傳認證格式錯誤
500,Other errors	其他錯誤	JSON 處理錯誤或未知錯誤
104,Access denied	存取權限錯誤	金鑰無法存取該設備感測器

◆ 上傳加密數據(認證加密)回傳結果

回傳格式: (字串)狀態碼,狀態描述(錯誤描述)

回傳資訊(String)	資訊說明	備註
0	OK	
406,Descrypt error	解密結果異常	
405,Incorrect checksum	Checksum 錯誤	CRC
410,Authentication error	認證錯誤	

411,Unauthenticated	未認證，或認證已失效 (24hr)	表示系統目前無存在認證結果，請重新進行雙向認證
407,ILLeage flag	Flag 異常	
104,Access denied	存取權限錯誤	金鑰無法存取該設備感測器

◆ 其他錯誤代碼

回傳格式: (字串)狀態碼,狀態描述(錯誤描述)

回傳資訊(String)	資訊說明	備註
101,Illegal topic	不存在(不允許)的 Topic	
102,ILLeage data	資料 JSON 格式不正確	
104,Access denied	存取權限錯誤	金鑰無法存取該設備感測器