台灣電力股份有限公司

AMI 通訊系統
P6 介面單元-KMS 與 MAM

版　　別：第　　版

總 頁 數： 18 頁 (含封面及附件)

文件編號：

中華民國 107 年 6 月 8 日

目錄

圖目錄

1. 前言

此文件描述 HES 伺服器與本公司後端系統之 KMS 及 MAM 的溝通方式，HES 需要進行如網路管理、金鑰更新等和後端連動之功能，本文件將描述 HES 如何和後端進行通訊、傳輸訊息內容格式以及不同應用情境時各欄位定義等，根據此文件實做可以讓 HES 和後端系統正確的接收、傳送相關資訊。

1.1. 範圍

本文件描述 HES 對後端系統所需要的功能與架構，如圖 1-1 HES 對後端系統定義範圍中的 P6 介面所示，本文件涵蓋 KMS 以及 MAM 的部份：

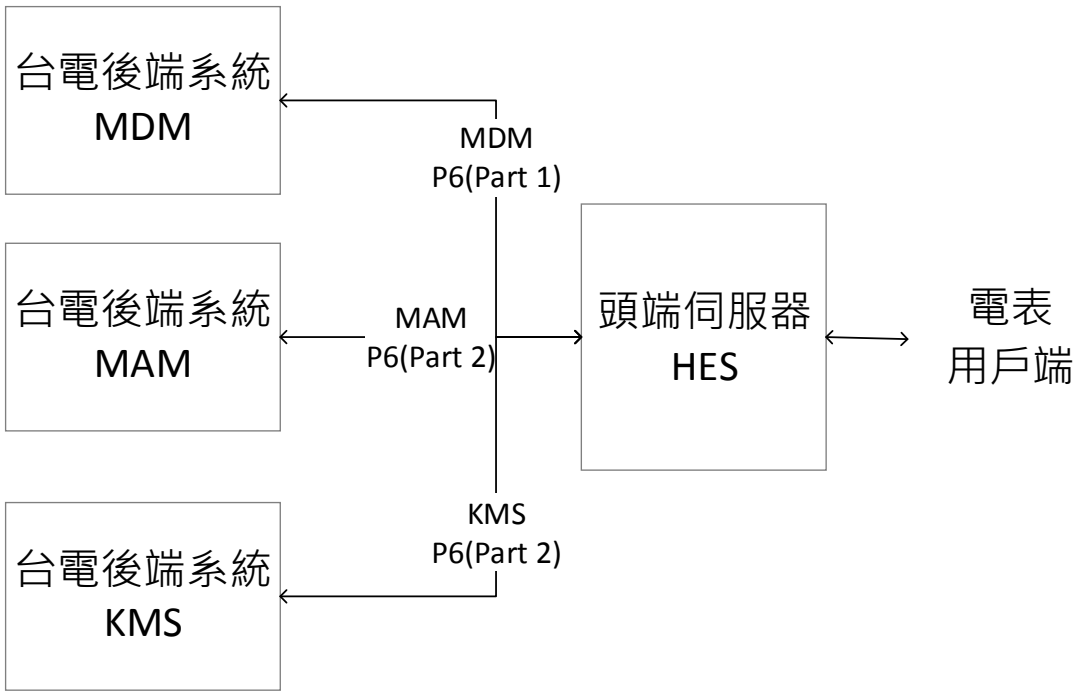


圖 1-1 HES 對後端系統定義範圍

1.2. 限制與前提

1. 後端系統與 HES 都需要有固定 IP，雙方需可透過此 IP 互相通訊。
2. 雙方均可開啟特定 Port 供連接使用。
3. 雙方皆可支援 HTTPS Restful 的 Client 及 Server 端的服務。

1.3. 參考標準資料

1.4. 術語與縮寫

1.4.1. 專有名詞定義

項目	定義
End Device	安裝在 HES 端之後的相關裝置，包含電表、IHD 或通訊裝置
Head End	接收電表資料並將其封裝成為 P6 格式與後端通訊的裝置
Premise area network	fully inclusive of the scope of a home area network (HAN) as it also covers commercial premises
PAN device	type of end device that is located on a customer premise and communicates using a PAN
MeterUniqueID	電表唯一識別碼，兩碼電表型式代號+8 碼的電表表號

1.4.2. 縮寫

縮寫	定義
HES	Head End System
MDM	Meter Data Management System
SOAP	Simple Object Access Protocol
JMS	Java Message Service
XML	Extensible Markup Language
IHD	In-Home Display
KMS	Key Management System
MAM	Meter Asset Manament System

2. 架構

2.1. 傳輸架構

HTTP Rest：雙方系統會過透過 HTTP 的 Client Server 架構來互傳訊息，若由 HES 發動的流程由 HES Client 送到後端 Server，若由後端 MAM/KMS 發動的流程由後端 Client 送到 HES Server 上，HTTP Rest 傳輸架構如下圖所示：

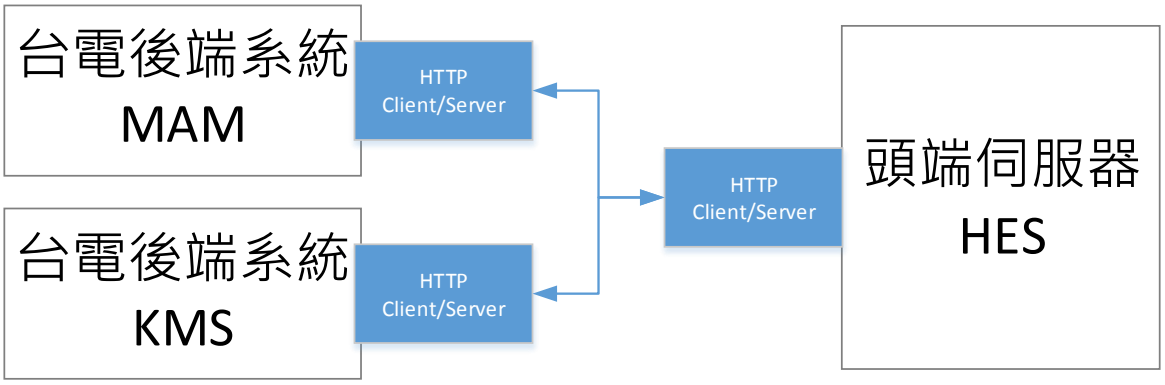


圖 2-1 後端 MAM/KMS 與 HES HTTP 通訊架構

2.2. 時間同步

為了維持讀表完整性，HES 與電表端的時間誤差需維持在 20 秒之內，而 HES 與後端系統之時間誤差不得超過 1 秒鐘，HES 與後端之時間同步需使用標準之 NTP v4 方式，此 NTP 伺服器由後端系統提供，HES 需設定指向此伺服器進行校時。

2.3. 服務 URL

由於本服務規格所訂定之傳輸訊息都已包含相關的指令、執行內容，所以在 KMS 端設為 https://[IP]:[port]/KMS，簡稱[KMS-URL]，MAM 端設為 https://[IP]:[port]/MAM，簡稱[MAM-URL]，HES 端需設為 https://[HES-IP]:[HES-Port]/HES，以下簡稱[HES-URL]，本服務內容皆採 TLS 加密，CA 由台電端提供。

2.4. Timeout

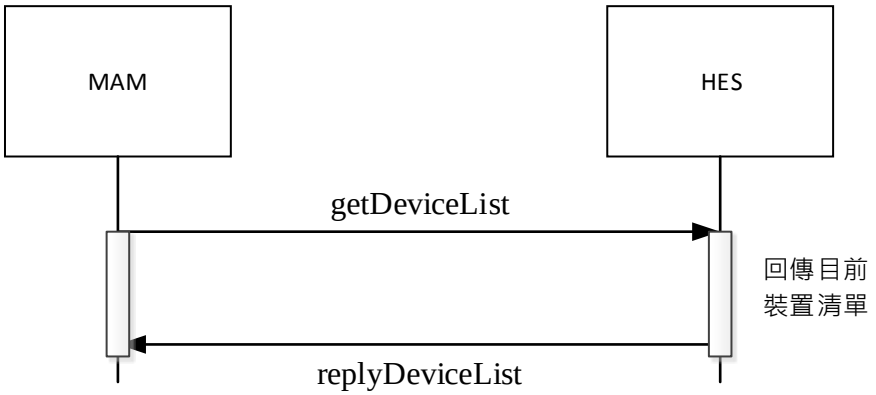
HTTPS 連線為 TCP 連線，當超過 timeout 訊息回應則會進行斷線並清除 session，Timeout 預設為 120 秒。

3. MAM 應用情境

應用情境描述 HES 對於後端系統以及對於底層系統的應對關係提供流程說明，不同的應用情境會對應到一個或多個傳輸指令，相關的指令將一一描述。

3.1. MAM 取得 AMI 系統裝置清單

此情境描述 MAM 端要取得 HES 系統下所管轄的裝置清單，在查詢時 HES 要回覆所管理的裝置清單。



- getDeviceList
- [QUERY]https://[HES-URL]/getDeviceList

```
{
   "time": "2017-01-01T00:00:00+0800",
   "session": "123e4567-e89b-12d3-a456-426655440000",
   "page": 10
}
```

項目	說明
time	訊息產生時間
session	為此訊息產生一筆 UUID
page	為了避免資料量大無法一次回傳，回應的數目以 1000 筆為限，每 1000 比稱為一頁(page)，page 從 1 開始，由 Query 時指定

- [RESPONSE]replyDeviceList

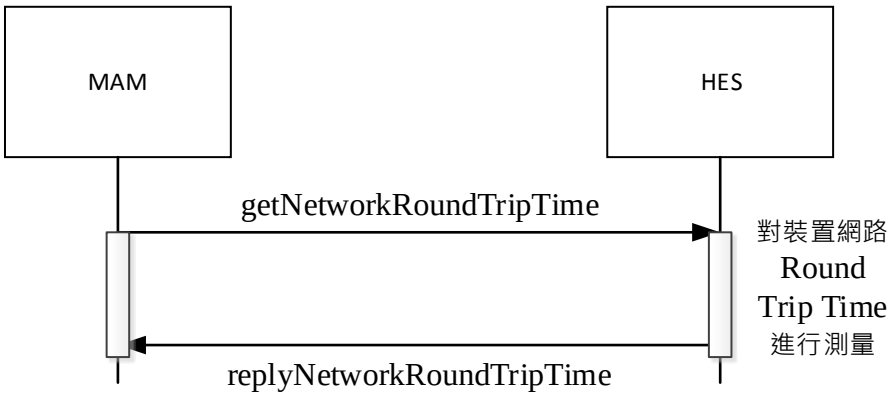
```
{
   "time": "2017-01-01T00:00:00+0800",
   "session": "123e4567-e89b-12d3-a456-426655440000",
   "total": 100000,
   "currentPage": 10,
   "device": [
      {
         "deviceId": "T012345678",
         "type": "Meter",
         "lat": 24.125454,
         "lng": 121.123131
      },
      {
         "deviceId": "41bb6ad6-1315-45ef-9d72-6c4a01d8961b",
         "type": "DCU",
         "lat": 24.125454,
         "lng": 121.123131
      }
   ]
```

```
}
```

項目	說明
time	訊息產生時間
session	須和 Query 的 session 對應
total	表示目前 HES 內有的裝置數量有多少
currentPage	為了避免資料量大無法一次回傳，回應的數目以 1000 筆為限，每 1000 比稱為一頁(page)，page 從 1 開始，由 Query 時指定，此欄位表示當前回應的資料是屬於哪個頁面，若是 Query 時給定的頁面不存在(如有 20000 筆資料但 page 指定 3)則此數字依然回傳 Query 的數字，但清單為空
device	● deviceId 裝置包含電表、FAN、Router 等等，此 ID 為裝置的編號，若是電表要使用 MeterUniqueID，若是其他裝置則 HES 端要自行產生一組固定的 UUID 來表示此裝置 ● type 裝置的型態，可為 Meter、FAN、Repeater、DCU、Router、HES 或是 Other ● lat 經緯度座標的緯度 ● lng 經緯度座標的經度

3.2. MAM 對裝置做網路 Round Trip Time 回應時間測試

此情境描述 MAM 要對 HES 系統下所的某個裝置進行 HES 到裝置端的網路 Round Trip Time 測試，概念類似於 IP 網路的 Ping 情境，由 HES 端發出一個 32 byte 的訊息並由裝置回應，測試網路是否有連通以及回應的時間長短，無論裝置有回應在 Timeout 時間到後都要回報



- getNetworkRoundTripTime
- [QUERY] https://[HES-URL]/getNetworkRoundTripTime

```
{
   "time": "2017-01-01T00:00:00+0800",
   "session": "123e4567-e89b-12d3-a456-426655440000",
   "timeout": 5,
   "device": [
      {
         "deviceId": "1e7868d7-8821-4f6d-9f54-7c6db5253d48"
      },
```

```
    {
      "deviceId": "41bb6ad6-1315-45ef-9d72-6c4a01d8961b"
    }
  ]
}
```

項目	說明
time	訊息產生時間
session	為此訊息產生一筆 UUID
timeout	從 HES 收到此訊息後要於多少時間內回應 MAM，單位為秒
device	裝置的 Array，裝置包含電表、FAN、Router 等等 ● deviceId 此 ID 為裝置的編號，若是電表要使用 MeterUniqueID，若是其他裝置則 HES 端要自行產生一組固定的 UUID 來表示此裝置

- [RESPONSE]replyNetworkRoundTripTime

```
{
  "time": "2017-01-01T00:00:00+0800",
  "session": "123e4567-e89b-12d3-a456-426655440000",
  "device": [
    {
      "deviceId": "1e7868d7-8821-4f6d-9f54-7c6db5253d48",
      "roundTripTime": 10
    },
    {
      "deviceId": "41bb6ad6-1315-45ef-9d72-6c4a01d8961b",
      "roundTripTime": null
    }
  ]
}
```

項目	說明
time	訊息產生時間
session	須和 Query 的 session 對應
device	裝置訊息 ● deviceId 對應 Query 的裝置 ID ● roundTripTime 為裝置的回應時間，以 ms 計算，以 FAN 為例是 HES 端到 FAN 之間的 round trip time，若是電表則是 HES 透過 FAN 端再由 FAN 發出 P1 的 Query 收到後回應到 HES 端的時間，若是 timeout 未回應則為 null

3.3. MAM 取得 AMI 系統裝置狀態

此情境描述 MAM 需要取得當前整個 AMI 的網路裝置狀態，希望得知每個節點上是否有連線不通、流量、拓撲等資訊，對網路的連線做一個評估

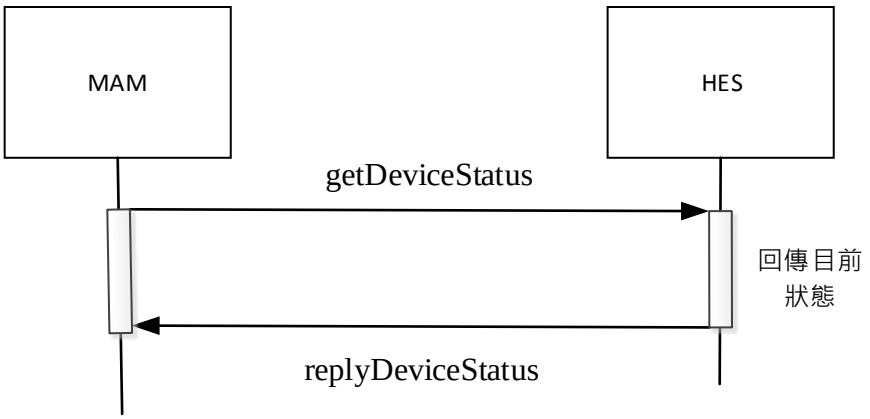


圖 3-1 後端取得 HES 狀態流程

- getDeviceStatus
  [QUERY]https://[HES-URL]/getDeviceStatus

```
{
   "time": "2017-01-01T00:00:00+0800",
   "session": "123e4567-e89b-12d3-a456-426655440000",
   "device": [
      {
         "deviceId": "T012345678",
         "dataFlow": {
            "timeStart": "2016-12-31T00:00:00+0800",
            "timeEnd": "2017-01-01T00:00:00+0800"
         },
         "deviceLog": {
            "timeStart": "2016-12-31T00:00:00+0800",
            "timeEnd": "2017-01-01T00:00:00+0800"
         }
      },
      {
         "deviceId": "e345057c-cd63-4746-8b4f-90eb62a619f2",
         "dataFlow": null,
         "deviceLog": null
      }
   ]
}
```

項目	說明
time	訊息產生時間
session	為此訊息產生一筆 UUID
device	Array 表示要讀取的 FAN、DCU/Base Station 等裝置，裝置使用唯一的 UUID 作為識別

dataFlow	timeStart 及 timeEnd 表示要取得的網路流量時間區段，通訊系統需要儲存最近 24 小時的資料，若不需要流量資料此欄位為 NULL
deviceLog	timeStart 及 timeEnd 表示要取得的 Log 時間區段，此訊息用於向 FAN 端取得 Security Gateway Log 使用，其他裝置若有填寫則無效，若不需要此訊息此欄位為 NULL

- [RESPONSE]replyDeviceStatus


```
{
   "time": "2017-01-01T00:00:00+0800",
   "session": "123e4567-e89b-12d3-a456-426655440000",
   "deviceStatus": [
      {
         "deviceId": "T012345678",
         "status": "offline",
         "updateTime": "2017-10-10T15:01:13+0800",
         "lastConnTime": "2017-10-10T15:01:13+0800",
         "parent": "e345057c-cd63-4746-8b4f-90eb62a619f2",
         "dataFlow": [
            {
               "port": "DCU LAN",
               "flow": [
                  {
                     "time": "2017-12-11T15:00:00+0800",
                     "txKbytes": 12313213,
                     "rxKbytes": 4816468
                  },
                  {
                     "time": "2017-12-11T15:15:00+0800",
                     "txKbytes": 7891321,
                     "rxKbytes": 23523
                  }
               ]
            },
            {
               "port": "DCU WAN",
               "flow": [
                  {
                     "time": "2017-12-11T15:00:00+0800",
                     "txKbytes": 12313213,
                     "rxKbytes": 4816468
                  },
                  {
                     "time": "2017-12-11T15:15:00+0800",
                     "txKbytes": 7891321,
                     "rxKbytes": 23523
                  }
               ]
            }
         ],
         "deviceLog": [
```

```
            {
               "time": "2017-12-11T15:00:00+0800",
               "message": "HAN read KWH "
            },
            {
               "time": "2017-12-11T15:01:00+0800",
               "message": "HAN block "
            }
         ]
      },
      {
         "deviceId": "e345057c-cd63-4746-8b4f-90eb62a619f2",
         "status": "online",
         "updateTime": "2017-10-10T15:01:13+0800",
         "lastConnTime": "2017-10-10T15:01:13+0800",
         "parent": "cac2fe38-08b5-43b0-a1b3-47edff53eb6e"
      }
   ]
}
```


項目	說明
time	訊息產生時間
session	須和 Query 的 session 對應
deviceStatus	Array 表示要回應的裝置資訊 ● deviceId 為電表的 MeterUniqueID 或是其他裝置的 UUID ● status 可為 online, offline ● updateTime 表示 status 取得的時間 ● lastConnTime 表示最近一次偵測到上線/連線的時間，可為 null ● parent 為網路節點上的上一層節點，電表和 FAN 視為不同的裝置，若為電表則上層是 FAN，若為 FAN 上層可能為 DCU 等，若為 mesh 可提供 routing 上一層的 FAN，編號由 HES 廠商自行定義之 UUID ● dataFlow 若有要求的話由 HES 端提供，依據不同的 port 來區分，比如 DCU 而言會有對後端以及對底 LAN 端的 port

4. KMS 應用情境

4.1. KMS 啟動金鑰更新/廢止

此情境描述當電表的金鑰需要更新或是電表的金鑰需要被廢止時由 KMS 發出一則訊息通知 HES 要將金鑰廢止或是進行更新金鑰的動作，在通知完後 HES 要開始進行金鑰更新，在更新完成後通知 KMS 端此金鑰已經更新。

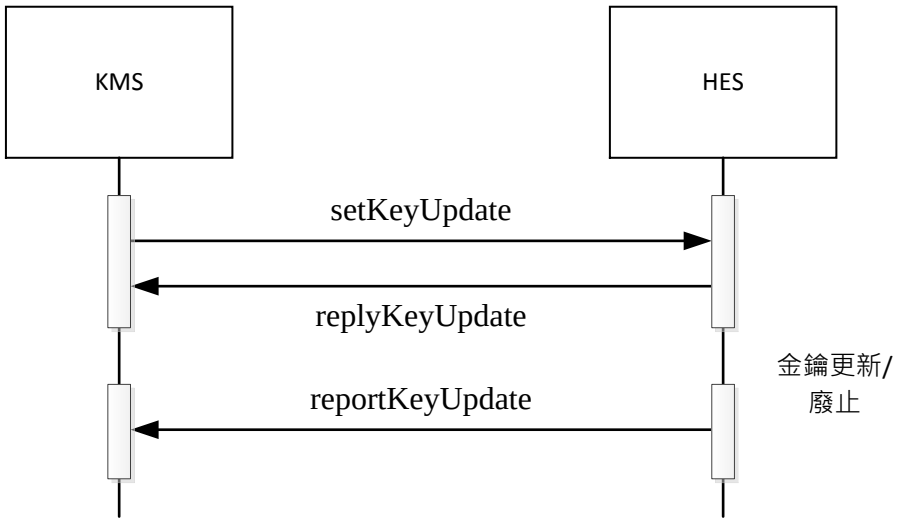


圖 4-1 KMS 通知 HES 金鑰更新/廢止流程

- setKeyUpdate
  [QUERY] https://[HES-URL]/setKeyUpdate

```
{
   "time": "2017-01-01T00:00:00+0800",
   "session":"123e4567-e89b-12d3-a456-426655440000",
   "meter":[
      {
         "deviceId": "T012345678",
         "command": "keyChange",
         "taskId": "3a74bc77-e338-432c-9965-46a7a93148de",
         "guk_mo": "AB338B47469051BA1E89C1F80434C7AB",
         "ak_mo": "6E9E2154592A9CFEE090354884B35471",
         "mk": "7BADF15E42539C0E4B6EF7165E3117E71F02BF9784ECA51D",
         "guk_m": "D94519555DBAFDD732D021017834D7151C83B734F3C86630",
         "ak_m": "B4C5904B8B8313667D4357F79DDF1C4F87CCF16F87EECEA1",
         "guk_h": "D168098012EF7012EA3A8ACBB27AA8AAB9D8E9439CD2BF1C",
         "ak_h": "C73A3EDC1BDB2EED1183A1F005CCF07B058F663F188C4214"
      },
      {
         "deviceId": "T012345679",
         "command": "keyDelete",
         "taskId": "ee3ab820-5787-4aa4-85cb-9d9c92da8502"
```

```
    }
  ]
}
```

項目	說明
time	訊息產生時間
session	為此訊息產生一筆 UUID
meter	Array 表示要更新或廢止金鑰的電表與命令 ● deviceId 為電表的 MeterUniqueID ● command 可為 keyChange, keyDelete ● taskId 為此次 setKeyUpdate 之 uuid ● guk_mo 表示當 command 為 keyChange 時，電表內的 Management client Global Unicast Key 的內容，無加密 ● ak_mo 表示當 command 為 keyChange 時，電表內的 Management client Authentication Key 的內容，無加密 ● mk 表示當 command 為 keyChange 時，要更新的 Master Key 加密後的內容 (可選) ● guk_m 表示當 command 為 keyChange 時，要更新的 Management client Global Unicast Key 加密後的內容 (可選) ● ak_m 表示當 command 為 keyChange 時，要更新的 Management client Authentication Key 加密後的內容 (可選) ● guk_h 表示當 command 為 keyChange 時，要更新的 HAN client Global Unicast Key 加密後的內容 (可選) ● ak_h 表示當 command 為 keyChange 時，要更新的 HAN client Authentication Key 加密後的內容 (可選)

- [RESPONSE]replyKeyUpdate

```
{
  "time": "2017-01-01T00:00:00+0800",
  "session":"123e4567-e89b-12d3-a456-426655440000",
  "received":true
}
```

項目	說明
time	訊息產生時間
session	須和 Query 的 session 對應
received	表示金鑰指令是否接收完畢，可為 true, false

- reportKeyUpdate
  [QUERY]https://[KMS-URL]/reportKeyUpdate

```
{
  "time": "2017-01-01T00:00:00+0800",
  "session":"550e8400-e29b-41d4-a716-446655440000",
```

```
  "meter":[
    {
      "deviceId": "T012345678",
      "result": true,
      "taskId": "3a74bc77-e338-432c-9965-46a7a93148de"
    },
    {
      "deviceId": "T012345679",
      "result": false,
      "taskId": "ee3ab820-5787-4aa4-85cb-9d9c92da8502"
    }
  ]
}
```

項目	說明
time	訊息產生時間
session	為此訊息產生一筆 UUID
meter	Array 表示更新或廢止金鑰的電表的處理結果 ● deviceId 為電表的 MeterUniqueID ● result 可為 true, false ● taskID 須和 setKeyUpdate 中各電表的 taskId 對應

4.2. HES 向 KMS 取得金鑰

此情境描述當 HES 有不知道電表金鑰的時候可以由 HES 端發出訊息去和 KMS 取得，KMS 會依據 HES 的來源確認是否可以合法提供此金鑰。

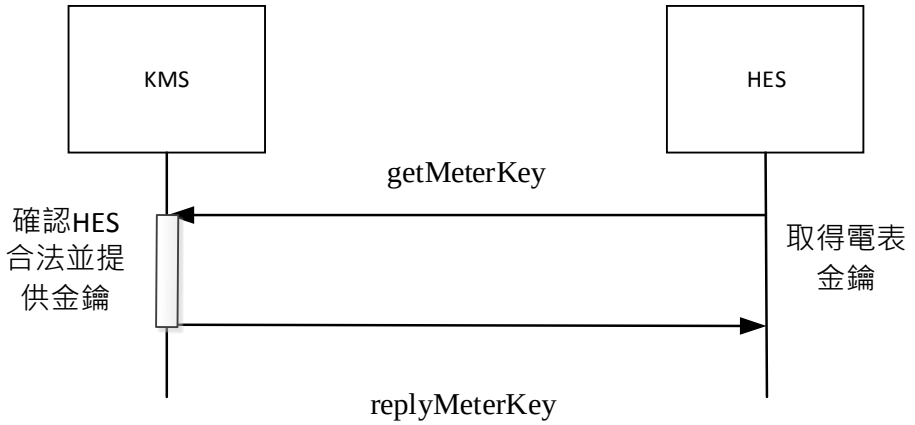


圖 4-2 HES 向 KMS 取得金鑰

- getMeterKey

[QUERY]https://[KMS-URL]/getMeterKey

```
{
   "time": "2017-01-01T00:00:00+0800",
   "session":"123e4567-e89b-12d3-a456-426655440000",
   "meter":[
      "T012345678",
      "T012345679"
      ]
}
```

項目	說明
time	訊息產生時間
session	為此訊息產生一筆 UUID
meter	Array 表示要索取金鑰的電表 MeterUniqueID

- [RESPONSE]replyMeterKey

```
{
   "time": "2017-01-01T00:00:00+0800",
   "session":"123e4567-e89b-12d3-a456-426655440000",
   "meter":[
      {
         "deviceId": "T012345678",
         "guk_m": "AB338B47469051BA1E89C1F80434C7AB",
         "ak_m": "6E9E2154592A9CFEE090354884B35471"
      },
      {
         "deviceId": "T012345679",
         "guk_m": "FAAFEA2A2963B963B1276B2AA46802E6",
         "ak_m": "870FC8B70478FFF275CC31CC86A91C01"
      }
   ]
}
```

項目	說明
time	訊息產生時間
session	須和 Query 的 session 對應
meter	Array 表示電表的與金鑰 ● deviceId 為電表的 MeterUniqueID ● guk_m 為電表內的 Management client Global Unicast Key 的內容，無加密 ● ak_m 為電表內的 Management client Authentication Key 的內容，無加密