聯邦銀行資料交換

雨芯有限公司一聯邦銀行

版本 VO.1

更新日期 2024/08/08

版本更新歷程

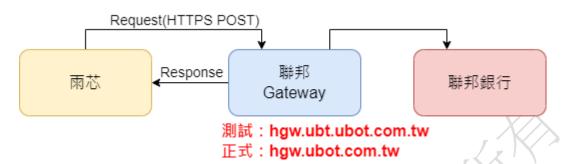
版本	更新內容摘要	頁碼	更新日期
V0. 1	初訂版	ALL	2024/08/08
			1/2
			, (()
		,	

目錄:

- I Online 即時查詢
 - 1. 虛擬代號即時明細查詢
- Ⅱ Notify 入帳通知
 - 1. 虛擬帳號入帳通知
- Ⅲ Batch 傳檔服務
 - 1. Sftp 虛擬帳號明細傳檔作業
- IV 加解密資訊
 - 1. HTTP 基本驗證機制 (Online 即時查詢)
 - 2. 加密流程與情境說明
 - 3. 加密作業說明
 - 4. 驗證作業說明
 - 5. 安控機制作業

I Online 即時查詢

1.虛擬代號即時明細查詢



Gateway 連線資訊

測試環境:https://hgw.ubt.ubot.com.tw/HGW/REST/BOARHAT

正式環境:https://hgw.ubot.com.tw/HGW/REST/BOARHAT

觸發條件:由企業戶端主動發起查詢 方式:HTTPS RESTful POST (JSON)

格式: Application/json UTF-8

驗證: POST with BASIC Authentication

ID: boarhat PWD:boarhat (測試)
ID: boarhat PWD:6dN3pAs0 (正式)

參數:請以 JSON 格式串成字串方式加入 Data 作為 Value

代號	名稱	長度	說明
txseq	交易序號	依貴方訂定	當日不重複序號
txcode	查詢代號	字串(07)	BOAQ001
acc	實體帳號	字串(12)	088100016711
sdate	實際交易起日	字串(08)	開始:01130808 民國
edate	實際交易迄日	字串(08)	結束:01130808 民國
stime	查詢起時間	字串(06)	開始:000000 時分秒
etime	查詢迄時間	字串(06)	結束:235959 時分秒
00000	虚擬代號	字串(03)	527
ecacc	19至19年1 人分元	子中(03)	左靠右補空白

BOAQ001

功能描述	虛擬代號-即時明細查詢 BOAQ001				
前端對象	雨芯有限公司				
URL Path	測試環境:https://hgw.ubt.ubot.com.tw/HGW/REST/BOARHAT				
	正式環境:https://hgw.ubot.com.tw/HGW/REST/BOARHAT				
HTTP	POST with BASIC Authentication				
Method	ID: boarhat PWD:boarhat (測試)				
	ID: boarhat PWD:6dN3pAs0 (正式)				
Request	JSON	. /.			
-	{"data":"{\"txseq\":\"0000001\",\"txcode\":\"BOAQ001\",\"	'acc\":\"088100016711\",\"			
	sdate\":\"01130808\",\"edate\":\"01130808\",\"stime\":\"000	0000\",\"etime\":\"235959\"			
	,\"ecacc\":\"527 \"}",				
	"mac":"Base64(AES128(Base64(SHA256(data))))",				
	"signature":"SHA256withRSA(mac)"				
	}				
	<u> </u>	V			
Response	單筆:				
	{"data":"				
	{\"txcode\":\"BOAQ001\",	//查詢代號			
	\"txseq\":\"00000001\",	//序號			
	\"data\":{\"T19D\":\" 01130808 01130808 140833 1486 8030123A74 0 2				

	\"}, //內容				
	\"msg\":\"\"}", //錯誤訊息內容				
	"mac":"Base64(AES128(Base64(SHA256(data))))",				
	"signature":"SHA256withRSA(mac)"				
_					
. 7					
X	多筆:				
X	{"data":"				
	{\"txcode\":\"BOAQ001\",	//查詢代號			
	\"txseq\":\"00000001\",	//序號			
	\"data\":[{\"T19D\":\" 01130808 01130808 140833 1486	8030123A74 0 2			
	**************1.00 918,356.00 803 52733-ATM				
	\"},{\"T19D\":\" 01130808 01130808 145409 14G6 803012				
	**************1.00 918,357.00 803 52733-EAI				
	\"}],	//內容			
	\"msg\":\"\"}",	//錯誤訊息內容			

```
"mac": "Base64( AES128( Base64( SHA256( data ) ) ) )",
"signature": "SHA256withRSA( mac )"
}
錯誤:
{"data":
\"txseq\":\"0000001\",
                                            //序號
\t''txcode\t'':\t''BOAQ001\t'',
                                            //查詢代號
\"data\":\"\",
                                            //內容
\"msg\":\"HT00M060 M060 查無此帳戶;無帳號或結清,移出超過兩年以上 \"}",
                                            //錯誤訊息內容
"signature":"",
"mac":""}
無資料:
{"data":
"{\"txseq\":\"00000001\",
                                            //序號
\"txcode\":\" BOAQ001\",
                                           //查詢代號
\"data\":\"查無明細資料\"
                                           //内容
\"msg\":\"\"}",
                                           //錯誤訊息內容
"signature": ""
"mac": ""
*内容為單筆 T19D 內容,請依下表進行資料內容取得
```

*紅字部分視為字串,進行 SHA、AES 加密及數位簽章;

BOAQ001 Data 內容欄位:

NO	FIELDS DESCRIPTION	TYPE/LENGTH	CONTENTS
8	下行 Data: BOAQ001 OUTPUT DATA 欄位說明:		
8.1	FORMID	X(04)	T19D
8.2	空白	X(01)	
8.3	銀行帳務日期	9(08)	Ex.01001201
8.4	空白	X(01)	
8.5	實際交易日期	9(08)	Ex.01001201
8.6	空白	X(01)	
8.7	交易時間	9(06)	Ex.173411
8.8	空白	X(01)	
8.9	交易代號	X(04)	Ex.14X5(註二)
8.10	空白	X(01)	
8.11	交易序號(機台+序號)	X(10)	Ex.9898900001
8.12	空白	X(01)	
8.13	交易狀態	X(01)	0:正常
			1:沖正
			9:錯誤刪除(此狀態不可顯
			示)
8.14	空白	X(01)	
8.15	交易類別	X(01)	1:借方(轉出)
			2:貸方(轉入)
			8:通知項(此類別不可顯示)
			9:濃縮項(此類別不可顯示)
8.16	空白	X(01)	
8.17	支出	X(17)	Ex.*****120,000.00
8.18	空白	X(01)	
8.19	收入	X(17)	Ex.*****120,000.00
8.20	空白	X(01)	
8.21	餘額	X(18)	Ex4,374,374.00
8.22	空白	X(01)	
8.23	對方銀行代號	X(03)	Ex.502
8.24	空白	X(01)	
8.25	交易摘要	X(10)	Ex.FXML 延轉
8.26	空白	X(01)	
8.27	摘要	X(16)	Ex.201007615ECT
0.27	加及	Λ(10)	(虛擬帳號後九碼 + ECT)

8.25 交易摘要說明

6.23 义勿恂安武明	
交易代號	中文說明
1200 · 1201	臨櫃現金支出
1290 \ 1291 \ \ 1220 \ \ 1221	臨櫃轉帳支出
1214 \ 1224	跨行ATM轉出(自行)
1227	跨行語音轉出
12E6	結購外幣
1215 \ 1225	跨行ATM轉出交易
12K3 12K4	晶片 自行繳費
12K5	晶片 跨行繳費
12K7	晶片 跨行繳稅
12J3 12J4	ID+ACCOUNT 自行繳費
12J5	ID+ACCOUNT 跨行繳費
12J7	ID+ACCOUNT 跨行繳稅
1228	自行語音轉出
1226	自行ATM轉出交易
1310 • 1370	轉帳繳款交易
12A5	FEDI 跨行扣帳
12S5	SET 跨行轉出
12A2	UMA 期貨轉出
1380	網路繳款交易
1400 · 1401	臨櫃現金存入
14X0	虛擬帳號現金存入
14Y0	虛擬帳號轉帳存入
1456 \ 1455	匯款存入
1480 • 1481	臨櫃轉帳存入
14K5	晶片 跨行繳費(入)
1484	ID+ACCOUNT 自行繳費入帳
14J5	ID+ACCOUNT 跨行繳費入帳
1486	自行ATM轉入
14E6	結售外幣
14I5、1485	跨行ATM轉入交易
1488	自行語音轉入
14A5	FEDI 跨行入帳
14X5	FXML 跨行轉入
14C5 14C7 14C8	eACH存入
14C6 14F6	ATM存現

14G6	電子存入
14A2	UMA 期貨轉入



Ⅱ Notify 主機發起通知

1.虚擬帳號入帳通知



正式:59.124.1.37、59.120.215.130

測試:124.219.117.124

通知目的:通知貴方帳戶即時入帳資訊 觸發條件:聯邦銀行主機端主動發起通知

虛擬代號:527

實體帳號:088100016711

通知 URL:請貴方協助提供 (測試):https:// 通知 URL:請貴方協助提供 (正式):https://

通知方式:HTTPS POST (JSON) 透通格式:Application/json UTF-8

虛擬帳號入帳通知內容

NO	FIELDS DESCRIPTION	LENGTH	CONTENTS
1	txseq	X(16)	序號 由 Gateway 定義建立
2	ubnotify	X(10)	通知代號 record (入帳通知)
3	to	X(03)	虛擬代號 527
4	acc	X(12)	實體帳號 088100016711
5	ecacc	X(14)	虛擬帳號 52733650000012
6	date	X(08)	交易日期 (西元年) 20240808
7	time	X(06)	交易時間 161214
8	amt	X(14)	交易金額 0000000124500 ->\$1245
٥	amt	二位小數點	文勿並領 0000000124300 ->\$1243
			交易狀態 0
9	status	X(01)	0:正向交易
			1:沖正交易
10	txnid	X(04)	交易代號 1486
11	stan	X(10)	交易識別碼 181000001
12	wdbank	X(03)	轉出銀行代號 803
13	wdacc	X(16)	轉出帳號 0000123456789012

功能描述	虛擬帳號-入帳通知
前端對象	雨芯有限公司 Web Service
URL Path	請貴方協助提供(測試):https://
UKL Patn	請貴方協助提供(正式):https://
HTTP	HTTPS POST
Method	11173 1031
	JSON
	{"data":"{\"txseq\":\"BOA000000000123\",\"ubnotify\":\"record\",\"to\":\"527\",
	lem:lem:lem:lem:lem:lem:lem:lem:lem:lem:
Request	\":\"161214\",\"amt\":\"00000000124500\",\"status\":\"0\",\"txnid\":\"1486\",\"stan\"
Request	:\"1810000001\",\"wdbank\":\"803\",\"wdacc\":\"0000123456789012\"}",
	"mac":"Base64(AES(Base64(SHA(data))))",
	"signature": "SHA256withRSA(mac)"
Response	{"txseq":"BOA00000000123","ubnotify":"record","resmsg":"success"}

^{*}紅字部分視為字串,進行 SHA、AES 加密及數位簽章;

txnid 交易代號對照表

交易代號 中文說明 1200、1201 臨櫃現金支出 1290、1291、1220、1221 臨櫃轉帳支出 1214、1224 跨行ATM轉出(自行) 1227 跨行語音轉出 1226 結購外幣 1215、1225 跨行ATM轉出交易 12K3 12K4 晶片 自行繳費 12K5 晶片 跨行繳費 12K7 晶片 跨行繳費 12J3 12J4 ID+ACCOUNT 自行繳費 12J5 ID+ACCOUNT 跨行繳費 12J7 ID+ACCOUNT 跨行繳稅 1228 自行語音轉出 1226 自行ATM轉出交易 1310、1370 轉帳繳款交易 12X5 FEDI 跨行扣帳 12X5 SET 跨行轉出 12A2 UMA 期貨轉出 1380 網路繳款交易 14V0 虛擬帳號現金存入 14X0 虛擬帳號現金存入 14X0 虛擬帳號轉帳存入 14X5 国片 跨行繳費(人) 1484 ID+ACCOUNT 自行繳費人帳 1455 ID+ACCOUNT 跨行繳費人帳 1486 自行ATM轉入 1486 自行ATM轉入 1486 自行ATM轉入 1488	txnid 父易代號對照表	
1290、1291、1220、1221 臨櫃轉帳支出 1214、1224 跨行ATM轉出(自行) 1227 跨行語音轉出 12E6 結購外幣 12I5、1225 跨行ATM轉出交易 12K3 12K4 晶片 自行繳費 12K5 晶片 跨行繳費 12K7 晶片 跨行繳費 12J4 ID+ACCOUNT 自行繳費 12J5 ID+ACCOUNT 跨行繳稅 12J7 ID+ACCOUNT 跨行繳稅 1228 自行語音轉出 1226 自行ATM轉出交易 14N5 1484 ID+ACCOUNT 跨行轉比 12A2 UMA 期貨轉出 1380 網路繳款交易 1400、1401 臨櫃現金存入 14X0 虛擬帳號現金存入 14X0 虛擬帳號現金存入 14K5 1484 ID+ACCOUNT 跨行繳費 (入) 1484 ID+ACCOUNT 跨行繳費 (入) 1486 自行ATM轉入 1486 自行ATM轉入 1488 自行ATM轉入 1488 自行语音轉入 1488 自行语音轉入 1488 自行语音轉入 1485 FEDI 跨行入帳 14X5 FXML 跨行轉人 14X5 FXML 跨行轉入 14X5 FXML B行轉入 14X5 FXML B行转入 14X5 FXML B介料 14X5	交易代號	中文說明
1214 \ 1224	1200 \ 1201	臨櫃現金支出
1227 跨行語音轉出 结購外幣 1215 \ 1225 跨行 A T M轉出交易 12K3 12K4 晶片 自行繳費 12K5 晶片 跨行繳稅 12K7 晶片 跨行繳稅 12J3 12J4 1D+ACCOUNT 自行繳費 12J5 1D+ACCOUNT 跨行繳稅 12J7 1D+ACCOUNT 跨行繳稅 1228 自行語音轉出 1226 自行 A T M轉出交易 13I0 \ 1370 轉帳繳款交易 12A5 FEDI 跨行扣帳 12S5 SET 跨行轉出 1380 網路繳款交易 1400 \ 1401 臨櫃現金存入 14X0 虛擬帳號現金存入 14X0 虛擬帳號現金存入 14K5 1481 臨櫃轉帳存入 1456 \ 1455 1284 1D+ACCOUNT 自行繳費入帳 14J5 1D+ACCOUNT 自行繳費入帳 14J5 1D+ACCOUNT 跨行繳費入帳 14B6 自行ATM轉入 14B6 自行ATM轉入 14B6 自行ATM轉入 14B6 自行ATM轉入 14B6 自行ATM轉入 14B8 自行語音轉入 14B8 自行語音轉入 14K5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14X5 FXML 跨行轉入 14X5 FXML 跨行轉入 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入 14C5 14C7 14C8 14C5 14C7 14C8 14C7 14C7 14C7 14C8 14C7 14C7 14C7 14C7 14C7 14C7 14C7 14C7 14	1290 · 1291 · 1220 · 1221	臨櫃轉帳支出
1215	1214 \ 1224	跨行ATM轉出(自行)
1215 \cdot 1225	1227	跨行語音轉出
12K3 12K4 晶片 自行繳費 12K7 晶片 跨行繳稅 12J3 12J4 ID+ACCOUNT 自行繳費 12J5 ID+ACCOUNT 跨行繳費 12J7 ID+ACCOUNT 跨行繳稅 1228 自行語音轉出 1226 自行A T M轉出交易 13I0、1370 轉帳繳款交易 12A5 FEDI 跨行扣帳 12S5 SET 跨行轉出 12A2 UMA 期貨轉出 1380 網路繳款交易 14V0 虛擬帳號現金存入 14X0 虛擬帳號轉帳存入 1456、1455 匯款存入 1480、1481 臨櫃轉帳存入 14K5 晶片 跨行繳費(入) 1484 ID+ACCOUNT 自行繳費入帳 14J5 ID+ACCOUNT 跨行繳費入帳 1486 自行ATM轉入 1486 自行ATM轉入 1486 自行ATM轉入 1488 自行語音轉入 1488 自行語音轉入 1485 跨行ATM轉入 1486 自行語音轉入 1487 FEDI 跨行入帳 1488 自行語音轉入 1489 自行語音轉入 1480 自行部音轉入 1481 EM	12E6	結購外幣
12K5 晶月 跨行繳費 12K7 晶月 跨行繳稅 12J3 12J4 ID+ACCOUNT 自行繳費 12J5 ID+ACCOUNT 跨行繳稅 12J7 ID+ACCOUNT 跨行繳稅 1228 自行語音轉出 1226 自行A TM轉出交易 1310、1370 轉帳繳款交易 12A5 FEDI 跨行扣帳 12S5 SET 跨行轉出 12A2 UMA 期貨轉出 1380 網路繳款交易 1400、1401 臨櫃現金存入 14X0 虛擬帳號轉長存入 14X0 虛擬帳號轉帳存入 14X0 塩櫃轉帳存入 14X0 塩櫃轉帳存入 14X5 晶片 跨行繳費(入) 14X5 日片ACCOUNT 自行繳費入帳 14X5 自行ATM轉入交易 1486 自行ATM轉入 14E6 結售外幣 14X5 跨行ATM轉入交易 1488 自行語音轉入 14X5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	1215 \ 1225	跨行ATM轉出交易
12K7 晶月 跨行繳稅 12J3 12J4 ID+ACCOUNT 自行繳費 12J5 ID+ACCOUNT 跨行繳稅 12J7 ID+ACCOUNT 跨行繳稅 1228 自行語音轉出 1226 自行A T M轉出交易 13I0、1370 轉帳繳款交易 12A5 FEDI 跨行扣帳 1285 SET 跨行轉出 12A2 UMA 期貨轉出 1380 網路繳款交易 1400、1401 臨櫃現金存入 14X0 虛擬帳號轉帳存入 1456、1455 匯款存入 1480、1481 臨櫃轉帳存入 14K5 晶片 跨行繳費(入) 1484 ID+ACCOUNT 自行繳費入帳 14J5 ID+ACCOUNT 跨行繳費入帳 1486 自行ATM轉入 1486 自行ATM轉入 1487 跨行ATM轉入交易 1488 自行語音轉入 14X5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	12K3 12K4	晶片 自行繳費
12J3 12J4	12K5	晶片 跨行繳費
12J5	12K7	晶片 跨行繳稅
12J7	12J3 12J4	ID+ACCOUNT 自行繳費
1228	12J5	ID+ACCOUNT 跨行繳費
1226	12J7	ID+ACCOUNT 跨行繳稅
1310 \ 1370	1228	自行語音轉出
12A5 FEDI 跨行担帳 12S5 SET 跨行轉出 12A2 UMA 期貨轉出 1380 網路繳款交易 1400、1401 臨櫃現金存人 14X0 虛擬帳號現金存入 14Y0 虛擬帳號轉帳存入 1456、1455 匯款存入 1480、1481 臨櫃轉帳存入 14K5 晶片 跨行繳費(人) 1484 ID+ACCOUNT 自行繳費入帳 14J5 ID+ACCOUNT 跨行繳費入帳 1486 自行ATM轉入 14E6 結售外幣 14I5、1485 跨行ATM轉入交易 1488 自行語音轉入 14A5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	1226	自行ATM轉出交易
12A2 UMA 期貨轉出 1380 網路繳款交易 1400、1401 臨櫃現金存入 14X0 虛擬帳號現金存入 14Y0 虛擬帳號轉帳存入 1456、1455 匯款存入 1480、1481 臨櫃轉帳存入 14K5 晶片 跨行繳費(人) 1484 ID+ACCOUNT 自行繳費入帳 14J5 ID+ACCOUNT 跨行繳費入帳 1486 自行ATM轉入 14E6 結售外幣 14I5、1485 跨行ATM轉入交易 1488 自行語音轉入 14A5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	1310 · 1370	轉帳繳款交易
12A2 UMA 期貨轉出 1380 網路繳款交易 1400、1401 臨櫃現金存入 14X0 虛擬帳號現金存入 14Y0 虛擬帳號轉帳存入 1456、1455 匯款存入 1480、1481 臨櫃轉帳存入 14K5 晶片 跨行繳費(人) 1484 ID+ACCOUNT 自行繳費入帳 14J5 ID+ACCOUNT 跨行繳費入帳 1486 自行ATM轉入 14E6 結售外幣 14I5、1485 跨行ATM轉入交易 1488 自行語音轉入 14A5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	12A5	FEDI 跨行扣帳
1380	12S5	SET 跨行轉出
1400、1401臨櫃現金存入14X0虛擬帳號現金存入14Y0虛擬帳號轉帳存入1456、1455匯款存入1480、1481臨櫃轉帳存入14K5晶片 跨行繳費(入)1484ID+ACCOUNT 自行繳費入帳14J5ID+ACCOUNT 跨行繳費入帳1486自行ATM轉入14E6結售外幣14I5、1485跨行ATM轉入交易1488自行語音轉入14A5FEDI 跨行入帳14X5FXML 跨行轉入14C5 14C7 14C8eACH存入	12A2	UMA 期貨轉出
14X0 虛擬帳號現金存入 14Y0 虛擬帳號轉帳存入 1456、1455 匯款存入 1480、1481 臨櫃轉帳存入 14K5 晶片 跨行繳費(入) 1484 ID+ACCOUNT 自行繳費入帳 14J5 ID+ACCOUNT 跨行繳費入帳 1486 自行ATM轉入 14E6 結售外幣 14I5、1485 跨行ATM轉入交易 1488 自行語音轉入 14A5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	1380	網路繳款交易
14Y0 虛擬帳號轉帳存入 1456、1455 匯款存入 1480、1481 臨櫃轉帳存入 14K5 晶片 跨行繳費(入) 1484 ID+ACCOUNT 自行繳費入帳 14J5 ID+ACCOUNT 跨行繳費入帳 1486 自行ATM轉入 14E6 結售外幣 14I5、1485 跨行ATM轉入交易 1488 自行語音轉入 14A5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	1400 • 1401	臨櫃現金存入
1456、1455匯款存入1480、1481臨櫃轉帳存入14K5晶片 跨行繳費(入)1484ID+ACCOUNT 自行繳費入帳14J5ID+ACCOUNT 跨行繳費入帳1486自行ATM轉入14E6結售外幣14I5、1485跨行ATM轉入交易1488自行語音轉入14A5FEDI 跨行入帳14X5FXML 跨行轉入14C5 14C7 14C8eACH存入	14X0	虛擬帳號現金存入
1480、1481臨櫃轉帳存入14K5晶片 跨行繳費(入)1484ID+ACCOUNT 自行繳費入帳14J5ID+ACCOUNT 跨行繳費入帳1486自行ATM轉入14E6結售外幣14I5、1485跨行ATM轉入交易1488自行語音轉入14A5FEDI 跨行入帳14X5FXML 跨行轉入14C5 14C7 14C8eACH存入	14Y0	虚擬帳號轉帳存入
14K5	1456 \ 1455	匯款存入
1484 ID+ACCOUNT 自行繳費入帳 14J5 ID+ACCOUNT 跨行繳費入帳 1486 自行ATM轉入 14E6 結售外幣 14I5、1485 跨行ATM轉入交易 1488 自行語音轉入 14A5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	1480 • 1481	臨櫃轉帳存入
14J5 ID+ACCOUNT 跨行繳費入帳 1486 自行ATM轉入 14E6 結售外幣 14I5、1485 跨行ATM轉入交易 1488 自行語音轉入 14A5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	14K5	晶片 跨行繳費(入)
1486 自行ATM轉入 14E6 結售外幣 14I5、1485 跨行ATM轉入交易 1488 自行語音轉入 14A5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	1484	ID+ACCOUNT 自行繳費入帳
14E6 結售外幣 14I5、1485 跨行ATM轉入交易 1488 自行語音轉入 14A5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	14J5	ID+ACCOUNT 跨行繳費入帳
14I5、1485 跨行ATM轉入交易 1488 自行語音轉入 14A5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	1486	自行ATM轉入
1488 自行語音轉入 14A5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	14E6	結售外幣
14A5 FEDI 跨行入帳 14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	14I5 \ 1485	跨行ATM轉入交易
14X5 FXML 跨行轉入 14C5 14C7 14C8 eACH存入	1488	自行語音轉入
14C5 14C7 14C8 eACH存入	14A5	FEDI 跨行入帳
	14X5	FXML 跨行轉入
14C6 14F6 ATM存現	14C5 14C7 14C8	eACH存入
	14C6 14F6	ATM存現

14G6	電子存入
14A2	UMA 期貨轉入



Ⅲ Batch 傳檔作業

1. Sftp 虛擬帳號明細傳檔作業



檔案命名:BOARHATSTRM.yyyyMMdd

備註:傳檔內容為傳檔當下的前一日 00:00:00-23:59:59 的交易資料明細,若無資料仍會產生空檔上傳,每日傳檔時間可能會因各公司時間誤差有些微差異,若貴方會每日定時讀檔,建議於聯邦傳檔時間延後 5-10 分鐘再進行收檔相關作業格式:請參閱「交易明細下傳格式」

== [測試] 雨芯傳檔伺服器連線資訊 ==

IP:請協助提供 Port:請協助提供 帳號:請協助提供 密碼:請協助提供 路徑:請協助提供

加密:ZIP 壓縮加密 密碼暫定 fD63o7V4yyyyMMdd

方式:SFTP 加密傳檔

作業名稱	上傳時間	上傳頻率	檔案名稱
虚擬帳戶 每日交易明細	(暫定) 上午 06:55	每日	BOARHATSTRM.yyyyMMdd

(上述 yyyyMMdd 皆為傳檔當日西元年月日,例:BOARHATSTRM.20240808)

交易明細下傳格式(FTP)

編號	項目名稱	項目長度	位置	備註
1	交易日期	9(08)	1	實際交易日
2	區隔符號	X(01)	9	· , ,
3	摘要	X(10)	10	虚擬帳號 5 碼+繳款方式(註一)
4	區隔符號	X(01)	20	·;'
5	摘要一	X(16)	21	(虛擬帳號後 9 碼+ECT)
6	區隔符號	X(01)	37	·;'
7	支出	9(17)	38	999999999999999999999999999999999999999
8	區隔符號	X(01)	55	·;'
9	存入	9(17)	56	999999999999999999999999999999999999999
10	區隔符號	X(01)	73	;
11	餘額	9(17)	74	-99999999999999999999999999999999999999
12	區隔符號	X(01)	91	
15	帳號	9(12)	92	99999999999
16	空白	X(02)	104	3

舉例:

(位置表示)

0 1 2 3 4 5 6 7 8 9

10

01030825;<mark>79683-TL</mark> ;(000029903ECT) ; ;00000000254869.00;

0000027950198.00;

註(一)繳款方式說明如下:

 -TL : 聯邦銀行臨櫃繳款
 -RM: 跨行匯款

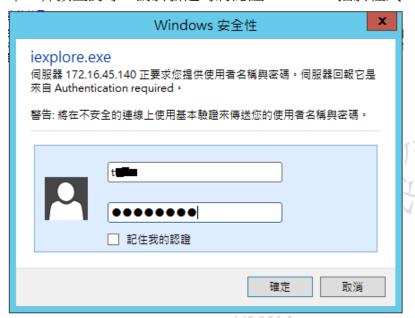
 -RT : 自行匯款
 -EB: 全國性繳費

-ATM: 自行 ATM 轉帳-CSH: 現金存款機存入-EAI: EAI 電子銀行轉入-ATMF: 跨行 ATM 轉帳

IV 加解密資訊

1.HTTP 基本驗證機制 (Online 即時查詢)

Gateway 中啟用 Basic authentication HTTP 認證功能,瀏覽器網頁驗證畫面如下所示;介接查詢等…請於發送時將認證 ID、PWD 描於程式 Header 中即可;



瀏覽器 REST 套件範例:



程式範例:

Java 擷取驗證時 Header 設定

HttpURLConnection.setRequestProperty("User-Agent", USER_AGENT);

HttpURLConnection.setRequestProperty("Content-Type", "application/json; charset=UTF -8");

HttpURLConnection.setRequestProperty("Authorization", "Basic Ym9hcmhhdDpib2Fya

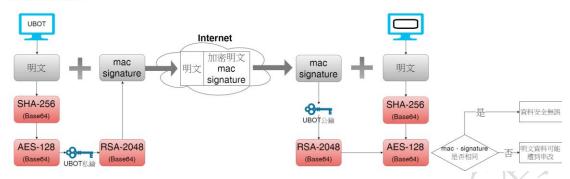
GF0 ");

BASE64 encoding

(ID:PWD)

2.加密流程與情境說明

上行加密驗證流程



範例 JSON:

{ "data":"上下行電文欄位內容",

"mac": "Base64(AES(Base64(SHA-256(data))))",

"signature": "SHA256withRSA(mac))"

mac:採 SHA-256、AES-128 加密,加密完後 Byte 轉 Base 結果顯示;AES 使用CBC/PKCS5Padding 加密與補碼方式,CBC 加密使用 IV、KeyFile 統一由聯邦銀行建立提供

signature:採 RSA-2048 數位簽章,簽章時使用己方私鑰,並提供對接單位公鑰 驗章時使用;

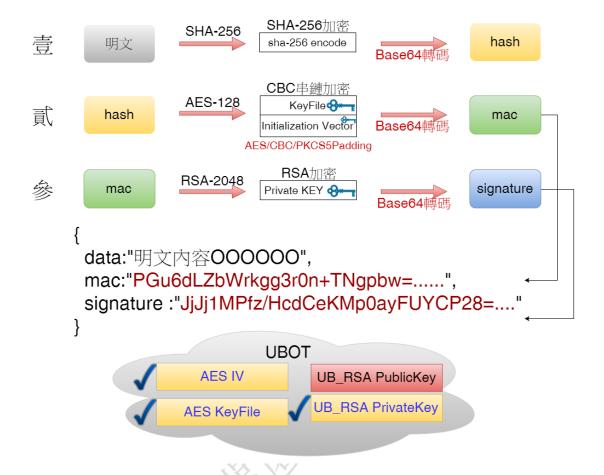
(加密驗證包含不可否認、不可竄改性)

RSA 公私鑰使用

作業	發起/驗證端	接收端	使用 Key
上行 Notify	UBOT	Company	UBOT_RSA_Private Key
驗證上行 Notify	Company		UBOT_RSA_Public Key
下行 Notify	Company	UBOT	
上行 Online	Company	UBOT	Company_RSA_Private Key
上行 Online 驗證上行 Online	Company UBOT	UBOT	Company_RSA_Private Key Company_RSA_Public Key
		UBOT Company	

(UB RSA Public Key 為 X509 Pem 格式)

3.加密作業說明



Ubot to Company 組成 JSON 上行加密過程

SHA-256:

- (1) 將明文 Data 內的資料,視為字串取出;
- (2) 將整段字串進行 SHA-256 加密後,取得整段 HashCode;
- (3) 將整段 HashCode 以 Base64 轉碼後,進入 AES 加密

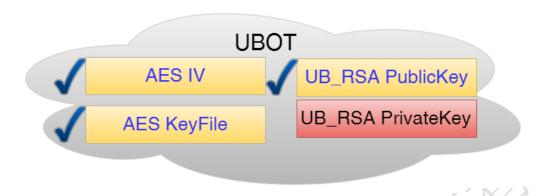
AES-128:

- (1) 使用聯邦銀行建立 UB RSA Public Key,將加密的 AES KeyFile 解密取出;
- (2) 將解密後的 AES KeyFile 及 Initialization vector(IV), 對剛 SHA-256 加密後的結果再進行 AES-128 加密;
- (3) 加密完成後以 Base64 轉碼後取得之加密內容,放入 JSON mac 欄位中 * AES 加密採 CBC/PKCS5Padding 方式

RSA-2048:

- (1) 利用聯邦銀行自己的 UB RSA Private Key,將 mac 進行數位簽章;
- (2) 將簽章值放入 JSON signature 欄位中;

4.驗證作業說明



驗證 Ubot 上行過程

檢查端:

signature : signature ---> Base64 decode ---> RSA verify --->mac,利用提供之公鑰驗章;

mac:明文—SHA256--->Base64--->AES CBC/PKCS5Padding--->Base64--->mac,將上 行端明文做加密(SHA-256)Base64 輸出,再進行 AES 加密後 Base64 輸出, 結果與上行 mac 比對完整性;

SHA-256:

- (1) 將明文 Data 內的資料,以字串方式取出;
- (2) 將整段字串進行 SHA-256 加密後,取得整段 HashCode;
- (3) 將整段 HashCode 以 Base64 轉碼後, 進入 AES 加密

AES-128:

- (1) 使用聯邦銀行提供 UB RSA Public Key,將加密的 AES KeyFile 解密;
- (2) 將解密後的 AES Key 及 Initialization vector(IV),對剛 SHA-256 加密後的 結果再進行 AES 加密;
- (3) 加密完成後以 Base64 轉碼後取得 mac;
- (4) 比對 mac 是否一致
- *AES 加密採 CBC/PKCS5Padding 方式

RSA-2048:

- (1) 將 signature 欄位內容取出;
- (2) 利用聯邦銀行提供 UB RSA Public Key 進行驗章;

5.安控機制作業

請務必先檢核 mac、signature 驗證通過後,方能信任 data 內文資料。 mac:含對稱式金鑰加密,雙方共用此金鑰,由銀行端產生提供; signature:為非對稱式金鑰簽/驗章,採私簽公驗,並雙方交換公鑰;

[Online 即時查詢]

(1) 銀行端設控連線 IP 白名單,如有更動請協助提出變更。

[Notify入帳通知]

- (1) 請檢核銀行端連線 IP。
- (2) 請確認 txseq 檢核當日不重複。
- (3) 請確認入帳虛擬帳號、金額與提供客戶繳款時相同。