TÀI LIỆU

****

HỆ THỐNG THANH TOÁN TRÁI PHIẾU PHÁT HÀNH RIÊNG LẺ - VCB C-BOND -

Tài liệu đặc tả kỹ thuật
Version: 0.5
Ngày: 12/06/2023

Hà Nội, ngày 12 tháng 06 năm 2023

Bảng theo dõi quá trình

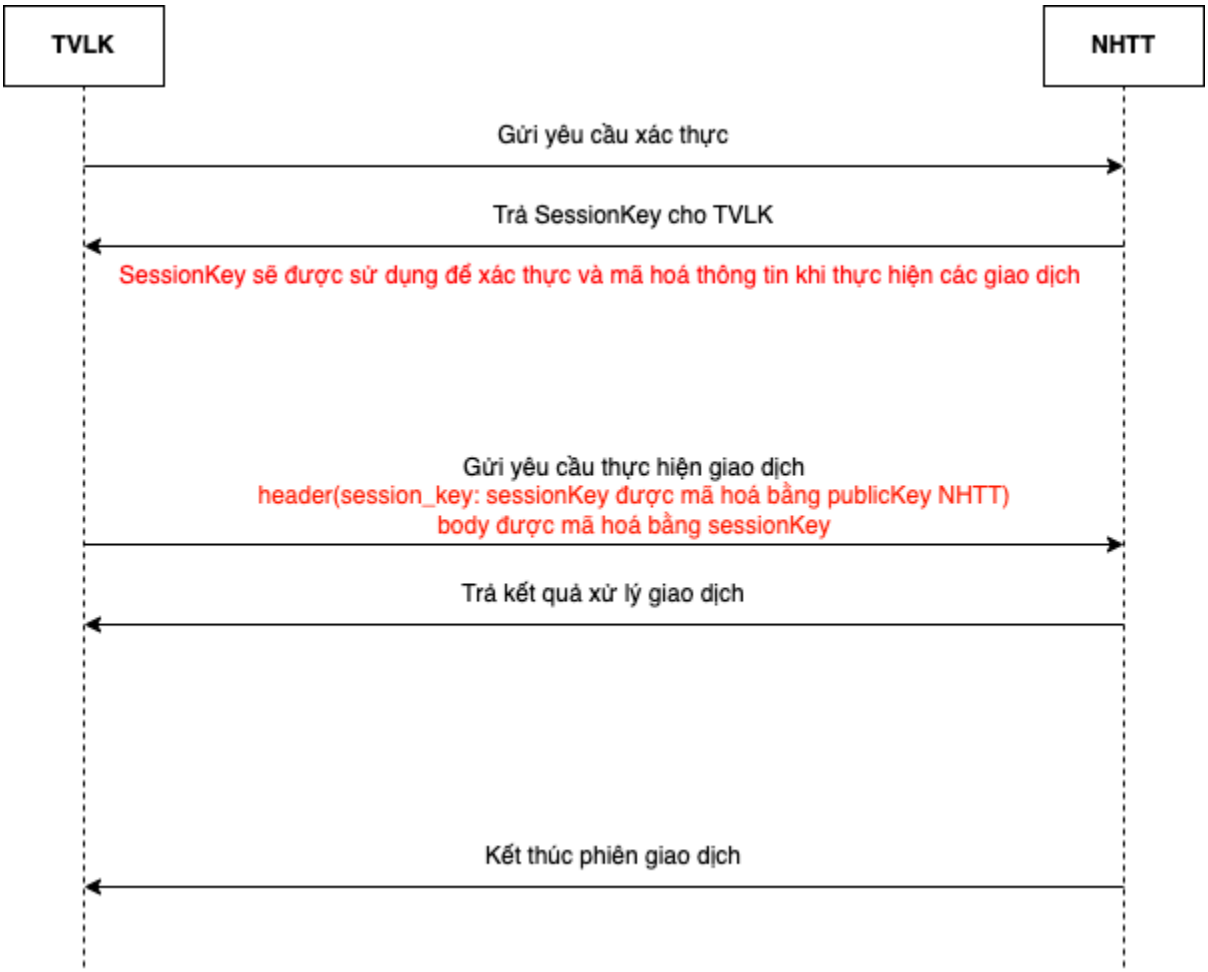
Cập nhật Tài liệu

Ngày	Phiên bản số	Ghi chú/Thay đổi	Người lập
22/05/2023	0.3	Khởi tạo	Nguyễn Minh Thơ Vũ Viết Quang
30/05/2023	0.4	Cập nhật thông tin: • Thêm quy định về mã Giao dịch Nộp/rút tiền • Thêm quy định về tên File báo cáo nhận về • Thêm chữ ký trong response của 2 API truy vấn thông tin NĐT và truy vấn kết quả giao dịch, TV có thể verify chữ ký để đảm bảo tính toàn vẹn của dữ liệu kết quả truy vấn nhận được • Thay đổi cơ chế nhận báo cáo: Sau cut-off nhận báo cáo của ngày T. Trước cut-off nhận báo cáo của ngày T-1. • Cập nhật thông tin mô tả 1 số trường rõ ràng hơn.	Nguyễn Minh Thơ Vũ Viết Quang
12/06/2023	0.5	Cập nhật thông tin: • Danh sách mã lỗi	Lê Ngọc Tuấn
…			
…			
…			
…			

TÀI LIỆU KỸ THUẬT
Mô tả API kết nối với TVLK

1. Mô hình kết nối

Dưới đây là mô hình kết nối trao đổi thông tin giữa Ngân hàng thanht toán và Thành viên lưu ký



2. Đường truyền kết nối

Thực hiện kết nối VPN site to site qua internet/leased line theo các thông tin sau (các thông tin cụ thể sẽ cung cấp sau khi có thỏa thuận kết nối được ký kết):

VPN Gateway Information:

Model	Thiết bị VPN S2S VCB	Thiết bị VPN S2S của đối tác
IP Address	DC: IP Public1 DR: IP Public2	
NATed	No	No

VPN Site-to-Site parameters:

Phase I	IKE version		
	IKE Encryption Algorithm		
	IKE Diffie-Hellman Group		
	IKE Hash Algorithm		
	Preshare key		
	Mode		
	Lifetime (second)		
Phase II	IPSEC Encryption Algorithm		
	IPSEC Hash Algorithm		
	Perfect Forward Secrecy		
	Life time (Second)		
	Support IP Compression		
	Tunnel Type		
	Traffic Selector (Proxy ID)	x.x.x.x	y.y.y.y

Connectivity Policy:

Application	Real Source	Nated Source	Real Destination	Nated Destincation	Port

3. Quy tắc chung về API

Yêu cầu về bộ Key:

- Thuật toán: RSA/ECB/OAEPWithSHA-256AndMGF1Padding , độ dài 2048 bit
- Mỗi thành viên cần có bộ Private/Public key để mã hóa/giải mã dữ liệu trao đổi với VCB.
- Tương tự, VCB cũng có bộ Private/Public Key để mã hóa/giải mã dữ liệu trao đổi với thành viên.
- Thành viên được VCB cấp 1 mã Secret Key dùng để xác thực với VCB và Public Key của VCB để mã hóa dữ liệu gửi cho VCB.
- Thành viên cung cấp Public Key của mình cho VCB để VCB mã hóa dữ liệu gửi về thành viên.

Ví dụ:

- Trong bản tin Request từ thành viên, thành viên mã hóa dữ liệu bằng Public Key của VCB. Chỉ VCB có PrivateKey của VCB nên đảm bảo dữ liệu chỉ có VCB có thể giải mã.
- Trong bản tin Response lại cho thành viên, VCB mã hóa dữ liệu bằng Public Key của thành viên. Chỉ thành viên có Private Key của mình nên đảm bảo dữ liệu chỉ thành viên có thể giải mã.

4. API xác thực thành viên

4.1 Mục đích

Cung cấp API để thành viên thực hiện xác thực và lấy token. Token lấy được sử dụng trong các request truy vấn thông tin và gửi giao dịch nộp rút tiền (thông tin biến động số dư tài khoản nhà đầu tư).

4.2 Thông tin yêu cầu đầu vào (Request)

URL: POST /public/api/v1/member/{memberCode}/login

Trường thông tin:

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú
bicCode	Biccode thành viên Biccode 8 ký tự tại VSD	Y	String	8	Mật khẩu là chuỗi Secret Key đã được mã hóa bằng Public Key của VCB
password	Mật khẩu	Y	String	512	

4.3 Thông tin đầu ra (Response)

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú
errorCode	Mã lỗi	Y	String		
errorDesc	Mô tả lỗi	Y	String		
transactionDate	Ngày GD	Y	Long		
result	Dữ liệu phản hồi	Y	Object		
memberCode	Mã thành viên	Y	String		Trường thông tin nằm trong result
sessionKey	Key dùng trong các bản tin request truy vấn, giao dịch. Đã được mã hóa bằng Public Key của thành viên. Cần giải mã bằng Private Key của thành viên để lấy thông tin Session Key dạng raw	Y	String		
expireDate	Thời điểm hết hạn	Y	Long		

4.4 Bản tin mẫu

Request:

```
{
  "bicCode": "VSDSSIXX",
```

"password": "HJThgbMjgIv.....d/6CTIAvpdANdOeOWfh40g9u=="
}

Response:
{
"errorCode": "00",
"errorDesc": "Success",
"transactionDate": 1680748804,
"result": {
"memberCode": "001",
"sessionKey": "W38HCCKiaaUsiKQ7P9B8UgbfkW.....+GA==",
"expireDate": 1680835203
}
}

5. API gửi thông tin giao dịch Nộp/Rút tiền

5.1 Mục đích

Thành viên gửi thông tin giao dịch nộp rút tiền của NĐT. Các giao dịch này sẽ được NHTT thực hiện hạch toán theo quy định của NHTT.

Bản tin phản hồi là thông tin giao dịch có được chấp thuận để đưa vào hàng đợi chờ hạch toán hay không. Không phải là kết quả hạch toán giao dịch. Thành viên tra cứu kết quả giao dịch theo API mô tả tại mục "API truy vấn kết quả giao dịch Nộp/Rút tiền" trong tài liệu này.

Nếu TV gửi giao dịch có mã trùng, sẽ nhận được thông báo lỗi và mã tham chiếu của giao dịch cũ.

5.2 Thông tin yêu cầu đầu vào (Request)

URL: POST public/api/v1/member/secure/{memberCode}/transaction
Header:

Tên Header	Giá trị
session_key	Session key dạng raw được mã hóa bằng Public key của VCB
Content-Type	application/json

Trường thông tin:

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú
bicCode	Biccode thành viên	Y	String	10	

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú
transactionNo	Mã giao dịch – duy nhất	Y	String	20	Quy ước: 3 ký tự đầu là Mã TV 6 ký tự tiếp là ngày hiện tại: yyMMdd 8 ký tự cuối là số tự tăng. Ví dụ: 00923052900000099
transactionType	Loại giao dịch	Y	Long		900 – Rút tiền 910 – Nộp tiền
transactionDate	Ngày giao dịch	Y	Long		Ngày giờ phải trong ngày hiện tại.
signature	Chữ ký.	Y	String	N	Chữ ký được ký bằng Private Key của TV
data	Dữ liệu	Y	String	N	Thông tin giao dịch, đã được mã hóa bằng Session Key dạng raw

Thuật toán mã hóa thông tin trường data**: AES/ECB/PKCS5Padding**

Thông tin trường data trước khi mã hóa:

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú
accountNo	Tài khoản nhà đầu tư tại thành viên	Y	String	10	TK 10 ký tự ví dụ 009Cxxxxxx
currency	Mã tiền tệ	Y	String	3	Giá trị: VND – Việt Nam đồng
amount	Số tiền giao dịch	Y	Long		Tối đa 15 ký tự
description	Mô tả	Y	String	256	

Định dạng chữ ký trước khi ký:

bicCode|transactionNo|transactionType|transactionDate|accountNo|currency|amount
Chữ ký trước khi ký được ghép bởi các trường dữ liệu dạng raw (không mã hóa)

5.3 Thông tin đầu ra (Response)

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú
errorCode	Mã lỗi	Y	String		
errorDesc	Mô tả lỗi	N	String		
transactionDate	Ngày GD	Y	Long		
result	Dữ liệu phản hồi	Y	String		Mã tham chiếu REFCODE giao dịch. Dùng để truy vấn kết quả giao dịch

4.4 Bản tin mẫu

Request:

{
"bicCode": "SSIXX",
"transactionNo": "TRANID--1244746321",
"transactionType": 900,
"transactionDate": 1680751011,
"signature": "BK6zvnG1y+b.....i/7nxGFNqI+My4GAQ==",
"data": "H4WlV+.....4XP7whUrql8SVbeVY7"
}

Trước khi mã hóa:

{
"bicCode": "SSIXX",
"transactionNo": "TRANID--1244746321",
"transactionType": 900,
"transactionDate": 1680751011,
"signature":"001C111333| VND|1000900"
"data":
{
"accountNo": "001C111333",
"currency": "VND",
"amount": 1000900,
"description": "test"

```
        }
}
```

Response:

```
{
   "errorCode": "00",
   "errorDesc": "Success",
   "transactionDate": 1680751028,
   "result": "80"
}
```

6. API truy vấn kết quả giao dịch Nộp/Rút

6.1 Mục đích

Truy vấn thông tin kết quả giao dịch dựa và số hiệu giao dịch. Giãn cách mỗi lần truy vấn 10s nếu nhận kết quả là đang chờ xử lý.

6.2 Thông tin yêu cầu đầu vào (Request)

URL: GET /public/api/v1/member/secure/{memberCode}/trans-status/{refCode}

Header:

Tên Header	Giá trị
session_key	Session key dạng raw được mã hóa bằng Public key của VCB
Content-Type	application/json

Trường thông tin: N/A

6.3 Thông tin yêu cầu đầu ra (Response)

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú
errorCode	Mã lỗi	Y	String		
errorDesc	Mô tả lỗi	N	String		
transactionDate	Ngày GD	Y	Long		
result	Dữ liệu phản hồi	Y	Object		

transactionNo	Mã GD của thành viên	Y	String		Trường thông tin nằm trong result. Danh sách trạng thái: 0 – Xử lý không thành công 1,2,3 – Đang xử lý 4 – Thành công
refCode	Mã tham chiếu của VCB	Y	String		
status	Trạng thái	Y	String		
description	Mô tả	N	String		
signature	Chữ ký	Y	String		

Định dạng chữ ký trước khi ký:
refCode|transactionNo|status
Chữ ký trước khi ký được ghép bởi các trường dữ liệu dạng raw (không mã hóa), ký bằng Private Key của VCB

6.4 Bản tin mẫu

Response:

```
{
   "errorCode": "00",
   "errorDesc": "Success",
   "transactionDate": 1680751977,
   "result": {
      "transactionNo": "TRANID--1244746321",
      "refCode": "74",
      "status": "4",
      "description": null,
      "signature": "Dp4V7Kj.....== "
   }
}
```

7. API tra cứu số dư Nhà đầu tư

7.1 Mục đích

Truy vấn thông tin số dư của NĐT tại thời điểm truy vấn. NHTT cung cấp API này để thành viên cập nhật thông tin số dư trước khi thực hiện các giao dịch mua/bán, giao dịch nộp/rút tiền cho NĐT.

7.2 Thông tin yêu cầu đầu vào (Request)

URL: GET /public/api/v1/member/secure/{memberCode}/get-balance/{account}
Header:

Tên Header	Giá trị

session_key	Session key dạng raw được mã hóa bằng Public key của VCB
Content-Type	application/json

Trường thông tin: N/A

7.3 Thông tin yêu cầu đầu ra (Response)

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú
errorCode	Mã lỗi	Y	String		
errorDesc	Mô tả lỗi	N	String		
transactionDate	Ngày GD	Y	Long		
result	Dữ liệu phản hồi	Y	Object		
accountNo	Tài khoản NĐT tại thành viên	Y	String		Trường thông tin nằm trong result.
accountType	Loại tài khoản theo thông tin VSD gửi về gồm: • Cá nhân trong nước DOMIND • Cá nhân nước ngoài FORIND • Tổ chức trong nước DOMCORP • Tổ chức nước ngoài FORCORP	Y	String		
amount	Số dư tại thời điểm truy vấn	Y	Long		
description	Mô tả	N	String		

signature	Chữ ký	Y	String		

Định dạng chữ ký trước khi ký:
accountNo|accountType|amount
Chữ ký trước khi ký được ghép bởi các trường dữ liệu dạng raw (không mã hóa), ký bằng Private Key của VCB

7.4 Bản tin mẫu

Response:

```
{
   "errorCode": "00",
   "errorDesc": "Success",
   "transactionDate": 1680752356,
   "result": {
      "accountNo": "001C111333",
      "accountType": "DOMIND",
      "amount": 94069999,
      "signature": "Dp4V7Kj.....== "
   }
}
```

8. Tra cứu giao dịch của NĐT tại NHTT

8.1 Mục đích

Gửi TVLK – Thống kê tất cả các giao dịch thanh toán trái phiếu theo điện VSD của TVLK
Tên File nhận được sẽ có định dạng: <Mã TV><Ngày><Mã báo cáo>.csv
Ví dụ: 0092023052909SQ01.csv

8.2 Thông tin yêu cầu đầu vào (Request)

URL: GET /public/api/v1/member/secure/{memberCode}/get-report/09SQ01
Header:

Tên Header	Giá trị
session_key	Session key dạng raw được mã hóa bằng Public key của VCB

Trường thông tin: N/A

8.3 Thông tin yêu cầu đầu ra (Response)

Hệ thống trả ra file CSV với các trường thông tin như sau:

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú

createdDate	Ngày	Y	Date		dd/MM/yyyy
refNo	Số REF của Điện thanh toán	Y	String		
memberCode	Mã TVLK	Y	String		
accNo	Số TK NĐT	Y	String		
orderType	Loại GD	Y	String		
debit	Phát sinh nợ	N	Long		
credit	Phát sinh có	N	Long		
remark	Nội dung	Y	String		
status	Trạng thái điện	Y	String		

9. Tra cứu số dư của NĐT tại NHTT

9.1 Mục đích

Gửi TVLK – Số dư tài khoản của tất cả các NĐT tại cuối mỗi ngày

9.2 Thông tin yêu cầu đầu vào (Request)

URL: GET /public/api/v1/member/secure/{memberCode}/get-report/09SQ02

Header:

Tên Header	Giá trị
session_key	Session key dạng raw được mã hóa bằng Public key của VCB

Trường thông tin: N/A

9.3 Thông tin yêu cầu đầu ra (Response)

Hệ thống trả ra file CSV với các trường thông tin như sau:

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú
createdDate	Ngày	Y	Date		dd/MM/yyyy
memberCode	Mã TVLK	Y	String		
accNo	Số TK NĐT	Y	String		
accType	Loại tài khoản	Y	String		
accNoRef	Số tài khoản P/C/F tương ứng	Y	String		
afbalance	Số dư cuối	Y	Long		

10. Tra cứu điện nộp/rút tiền của NĐT tại TVLK

10.1 Mục đích

Gửi TVLK – Thống kê tất cả các điện nộp/rút tiền của TVLK

10.2 Thông tin yêu cầu đầu vào (Request)

URL: GET /public/api/v1/member/secure/{memberCode}/get-report/09SQ03

Header:

Tên Header	Giá trị
session_key	Session key dạng raw được mã hóa bằng Public key của VCB

Trường thông tin: N/A

10.3 Thông tin yêu cầu đầu ra (Response)

Hệ thống trả ra file CSV với các trường thông tin như sau:

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú
orderDate	Ngày	Y	Date		dd/MM/yyyy
orderTime	Giờ nhận điện	Y	String		

memberCode	Mã TVLK	Y	String		
accNo	Số TK NĐT	Y	String		
orderType	Loại giao dịch	Y	String		
debit	Phát sinh nợ	N	Long		
credit	Phát sinh có	N	Long		
description	Nội dung	Y	String		
orderNo	Số REF của điện	Y	String		
status	Trạng thái điện	Y	String		

11. API thay đổi Secret Key

11.1 Mục đích

Thành viên đổi Secret Key được cấp phát

11.2 Thông tin yêu cầu đầu vào (Request)

URL: POST public/api/v1/member/secure/{memberCode}/change

Header:

Tên Header	Giá trị
session_key	Session key dạng raw được mã hóa bằng Public key của VCB
Content-Type	application/json

Trường thông tin:

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú
bicCode	Biccode thành viên	Y	String	10	
secretKey	Secret Key cũ	Y	String	N	Mật khẩu cũ, được mã hóa bằng Public Key của VCB
newSecretKey	Secret Key mới	Y	String	N	Mật khẩu mới, được mã hóa bằng Public Key của VCB
signature	Chữ ký.	Y	String	N	Chữ ký được ký bằng Private Key của TV

Định dạng chữ ký trước khi mã hóa: **secretKey|newSecretKey**
Chữ ký trước khi ký được ghép bởi các trường dữ liệu dạng raw (không mã hóa)

11.3 Thông tin đầu ra (Response)

Tên trường	Mô tả	Bắt buộc	Kiểu dữ liệu	Độ dài	Ghi chú
errorCode	Mã lỗi	Y	String		
errorDesc	Mô tả lỗi	N	String		
transactionDate	Ngày GD	Y	Long		
result	Dữ liệu phản hồi	Y	String		Trong trường hợp này dạng String

11.4 Bản tin mẫu

Request:

{
"bicCode":"VSDVCBSX",
"secretKey":"DVbyuud...8uy==",
"newSecretKey":"JK9xvs...w==",
"signature":"ZxvGu...QFGew9cw=="
}

Response:

{
"errorCode": "00",
"errorDesc": "Success",
"transactionDate": 1680751028,
"result": "00"
}

12. Phụ lục: bảng mã lỗi tích hợp

Mã lỗi	Mô tả
00	Thành công
01	Thông tin nghiệp vụ trong điện không hợp lệ
02	NĐT không tồn tại
03	NĐT không đủ số dư
06	Không tìm thấy TK thành viên
30	NĐT có lệnh chờ thanh toán
40	Thông tin thành viên không hợp lệ
41	Định dạng STK NĐT không hợp lệ
42	NĐT không thuộc thành viên
54	Ngày giao dịch không hợp lệ
55	Phiên không hợp lệ
60	Phiên đã kết thúc, dừng hạch toán
61	Phiên đã kết thúc, không nhận giao dịch
62	Thông tin mã hóa không hợp lệ
63	Thông tin chữ ký không hợp lệ
66	Session expired
77	UnAuthorize

90	Mã giao dịch trùng
91	Loại giao dịch không hợp lệ
92	Thông tin không hợp lệ
93	Số tham chiếu không được phép truy vấn
95	Lỗi hạch toán trên Corebanking
96	Gửi File tới VSD thất bại
97	Lỗi lưu Log điện phản hồi
98	Lỗi chuyển định dạng điện
99	Lỗi xử lý. Vui lòng liên hệ Quản trị hệ thống