DỊCH VỤ VNPT-SMARTCA

Tài liệu đặc tả và hướng dẫn tích hợp

Version 1.0

VNPT, 2021
Tòa nhà Internet, Lô 2A, Làng Quốc tế Thăng Long, Cầu Giấy, Hà Nội

Công ty Công Nghệ Thông Tin VNPT
Lô 2A, làng Quốc tế Thăng Long
Cầu Giấy, Hà Nội

Điện thoại 18001260

Website https://smartca.vnpt.vn

Email nguyendanghuy@vnpt.vn

Phiên bản tài liệu 1.0.0

Ngày phát hành 22-08-2021

Trạng thái tài liệu Hoàn thành

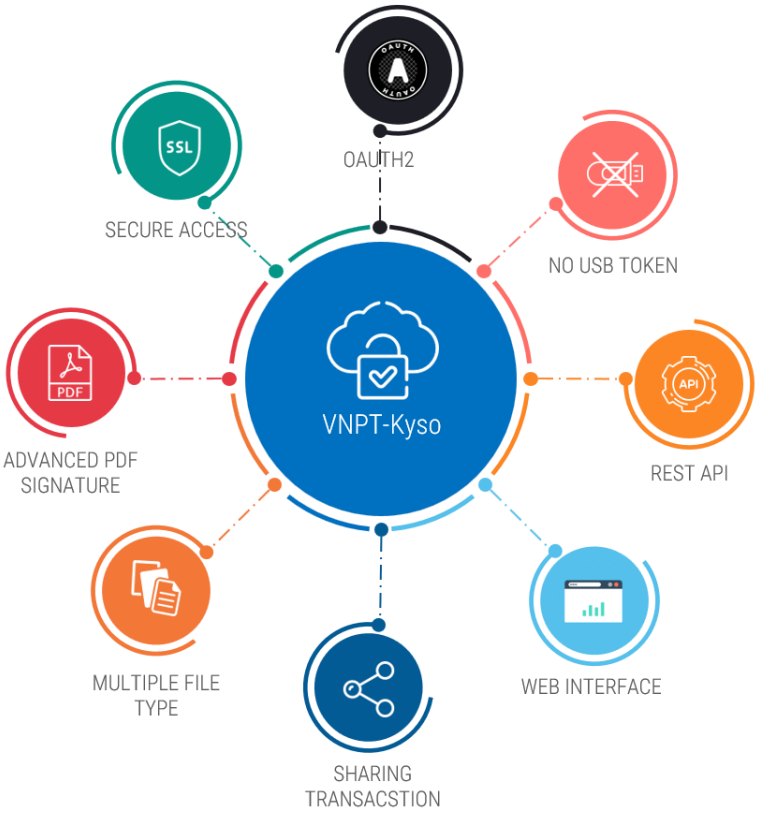
Lịch sử sửa đổi

Ngày sửa đổi	Người thực hiện	Nội dung
22/08/2021	Bùi Sĩ Tuấn	Initial document

MỤC LỤC

1 Giới thiệu

Cảm ơn quý khách đã tin tưởng sử dụng **Dịch vụ VNPT SmartCA**.



Thông tin tổng quan và giới thiệu về giải pháp, vui lòng xem thêm trong tài liệu Giới thiệu giải pháp **VNPT-SmartCA Solution Introduction**

Vui lòng liên hệ với chúng tôi nếu có bất cứ câu hỏi hoặc góp ý nào liên quan đến dịch vụ.

1.1 Thông tin tài liệu

Tài liệu này mô tả phân hệ **VNPT-SmartCA API Gateway**, cổng dịch vụ cho phép đối tác kết nối và thực hiện các nghiệp vụ liên quan đến chữ ký số thông qua giao diện web service.

1.2 Quy ước sử dụng

Trong tài liệu này chúng tôi sử dụng các quy ước sau nhằm giúp việc trình bày được rõ ràng và thuận tiện hơn trong việc nắm bắt nội dung:

Quy ước	Ý nghĩa	Ví dụ
`Courier New`	Đoạn code	`"RequestID": "5b483845-35b6-48c9-b9a6-3a4024271271"`
Bold	Nội dung cần nhấn mạnh	…yêu cầu phương thức **POST**.
`code`	Tham số hoặc giá trị tham số, kết quả	`response type=code`

Các nội dung cần lưu ý sẽ được trình bày với định dạng như sau:

Nội dung cần lưu ý

2 Giao thức API

Phân hệ Gateway API được cung cấp qua giao thứ **HTTPs** và yêu cầu phương thức **POST**.

Tham số sử dụng cho tất cả request vào protected resource service có định dạng **application/json**.

	Demo	Production
Địa chỉ authorization service	https://rmgateway.vnptit.vn/auth/authorize	https://gwsca.vnpt.vn/auth/authorize
Địa chỉ yêu cầu access_token	https://rmgateway.vnptit.vn/auth/token	https://gwsca.vnpt.vn/auth/token
Địa chỉ protected resource service	https://rmgateway.vnptit.vn	https://gwsca.vnpt.vn

3 Token Authorization

Nhằm bảo vệ chữ ký số cùng các thông tin của người dùng, đồng thời xác thực người dùng, xác thực ứng dụng bên thứ 3 thực hiện giao dịch. VNPT SmartCA ứng dụng mô hình xác thực dựa trên token (Token base Authorization).

Hệ thống xác thực được xây dựng theo giao thức Oauth2 (RFC 6479) cung cấp 2 mô hình xác thực:

- Authorization code
- Resource Owner Password Credentials

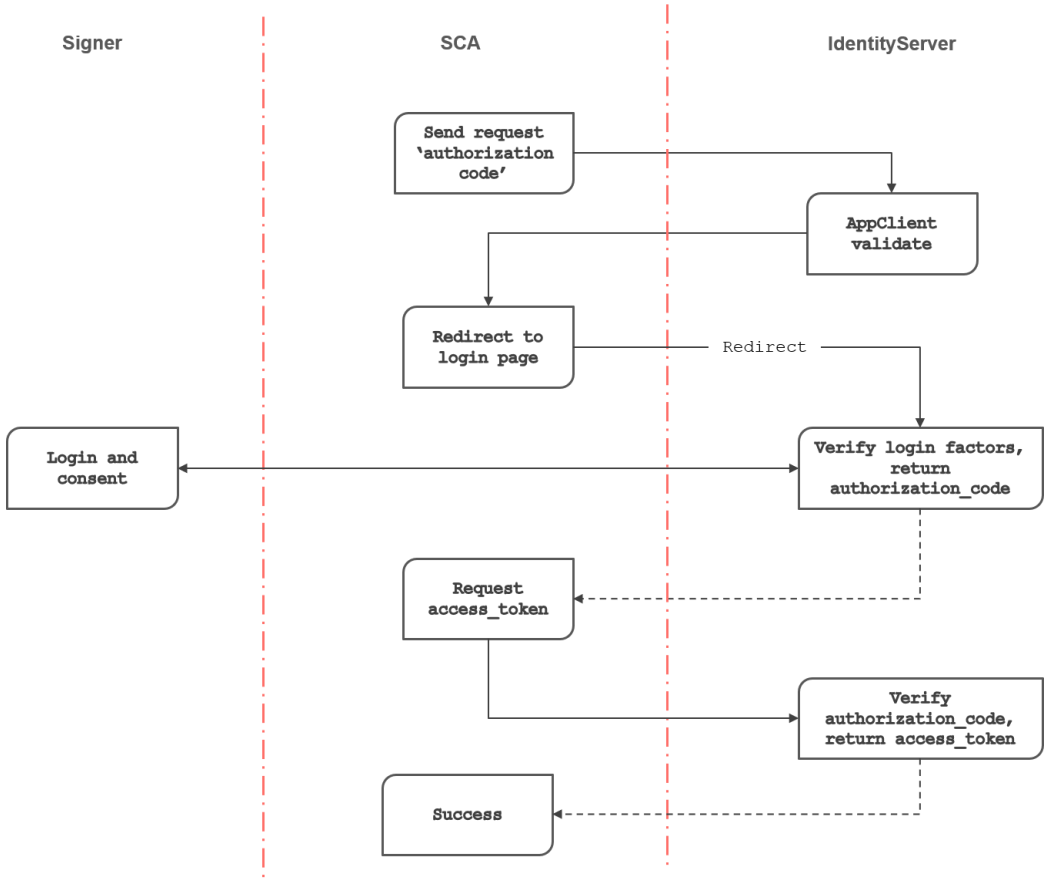
Người dùng (chủ sở hữu chữ ký số tập trung) được định danh bởi cặp thông tin **uid, password.**

Ứng dụng muốn lấy các thông tin người dùng hoặc gửi yêu cầu ký số bắt buộc phải có sự đồng ý của người dùng. Sau khi xác thực thông tin tài khoản với VNPT SmartCA, người dùng sẽ đồng ý cấp quyền để ứng dụng có thể đọc các thông tin public cũng như gửi yêu cầu ký số.

Sau khi đối tác (khách hàng doanh nghiệp) đăng ký sử dụng API sẽ trở thành Nhà phát triển, cho phép đăng ký và quản lý các ứng dụng được phép kết nối tới API.
Xem thêm tài liệu giới thiệu giải pháp **VNPT SmartCA Solution Introduction**

3.1 Authorization code

Phù hợp với tất cả các ứng dụng web hoặc native application. Người dùng sẽ xác thực trực tiếp với VNPT SmartCA và đồng ý cấp quyền để ứng dụng sử dụng Protected resource của mình (gửi yêu cầu ký số).



Bước 1: Ứng dụng gửi yêu cầu Authorization code tới VNPT-SmartCA

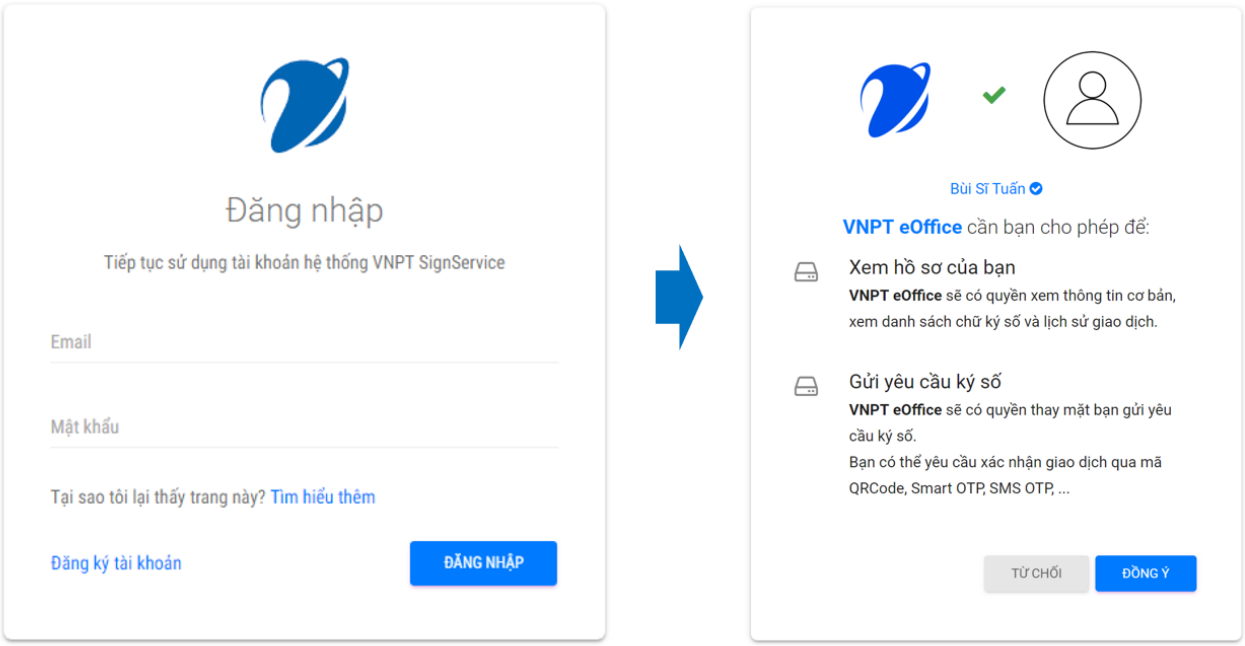
Authorize request:

- URL DEMO: https://rmgateway.vnptit.vn/auth/authorize
- URL PRODUCTION: https://gwsca.vnpt.vn/auth/authorize
- HTTP Method: **POST**
- HTTP Content-Type: **x-www-form-urldencoded**
- HTTP Body parameter:

Key	Type	Description
response_type	String	Yêu cầu giá trị là code
client_id	String	Định danh ứng dụng client
state	String	Giá trị sẽ được trả nguyên vẹn khi redirect về từ dịch vụ. Có thể sử dụng với 2 mục đích • Lưu dữ liệu người dùng ngay cả khi bị redirect • Chống tấn công CSRF
redirect_uri	String	Callback url để dịch vụ gọi lại gửi giá trị authorization_code (yêu cầu cấu hình trước)
scope	String	Yêu cầu giá trị là sign offline_access

VNPT SmartCA trả về cho ứng dụng một **redirect response** yêu cầu ứng dụng chuyển hướng người dùng đến trang đăng nhập của VNPT SmartCA

Bước 2: Ứng dụng chuyển hướng người dùng đến trang đăng nhập của VNPT SmartCA, người dùng đăng nhập sử dụng tài khoản VNPT SmartCA và cấp quyền truy cập cho ứng dụng.



Bước 3: VNPT-SmartCA sẽ trả giá trị gọi hàm callback của ứng dụng thông qua tham số redirect_uri dưới dạng

- URL: <redirect_uri>?code=<access_token_exchange_value>&state=<client_values>
- HTTP Method: GET

Tham số **code** trả về dùng để trao đổi access_token trên hệ thống VNPT SmartCA, tham số **state** dùng để kiểm tra với tham số đã truyền trong request ở bước trước.

- Tham số **code** chỉ có hiệu lực trong thời gian **15 giây** kể từ khi response được gửi về ứng dụng.
- **redirect_uri** yêu cầu trùng với uri đã đăng ký

Bước 4: Ứng dụng sử dụng tham số code để yêu cầu access_token

Token request:

- URL DEMO: https://rmgateway.vnptit.vn/auth/token
- PRODUCTION: https://gwsca.vnpt.vn/auth/token
- HTTP Method: `POST`
- HTTP Content-Type: `x-www-form-urldencoded`
- HTTP Body paramter:

Key	Type	Description
`grant_type`	String	Yêu cầu giá trị là `authorization_code`
`client_id`	String	Định danh ứng dụng client

client_secret	String	Chuỗi giá trị bí mật tương ứng với ứng dụng client
code	String	Giá trị trả về từ bước 3
redirect_uri	String	Callback url để dịch gọi lại gửi giá trị access_token (yêu cầu cấu hình trước)

Bước 5: VNPT-SmartCA trả về response chứa access_token, refresh_token và các thông tin bổ sung cho ứng dụng

Token response:

- HTTP Content-Type: **application/json: charset=utf-8**
- HTTP Body response:

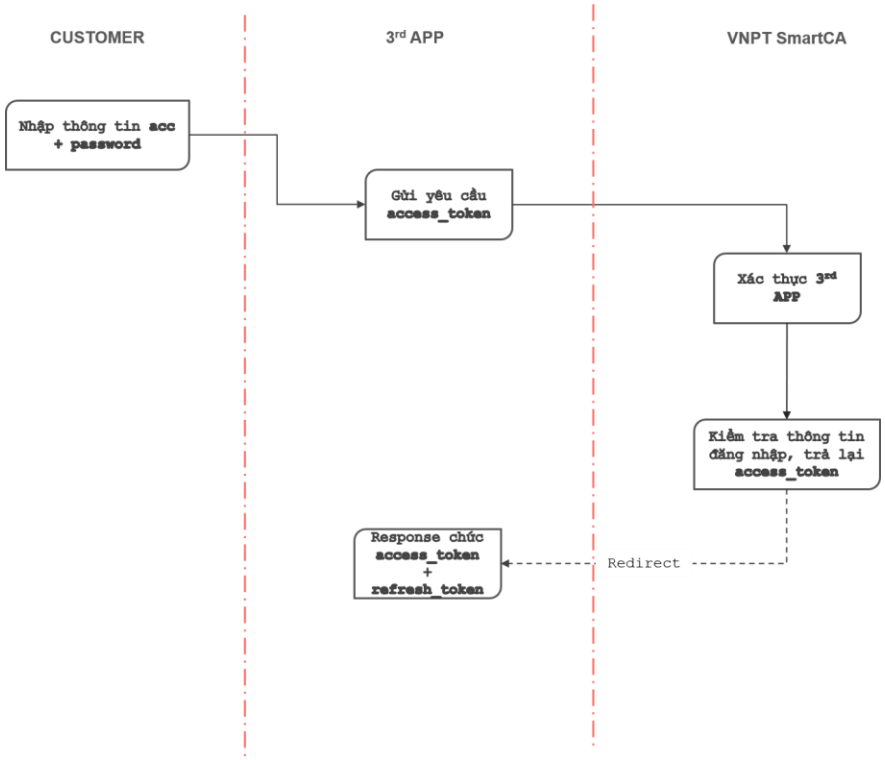
Key	Type	Description
access_token	String	Giá trị access_token định dạng JWT
refresh_token	String	Giá trị refresh_token dùng để yêu cầu access_token mới khi hết hạn.
token_type	String	Định dạng token. Mặc định là `bearer`
expires_in	String	Thời gian hiện lực của access_token tính bằng giây
scope	String	Thông tin các access mà access token này được cấp

- Mẫu response

```
{
    "access_token": "eyJ0eXAiOiJKV1QiLCJhbGc...",
    "refresh_token": "dV5o7erpj/GCdWAW2zQkcLsiX0bUUYSLGhwa4d7BIKE="
    "token_type": "bearer",
    "expires_in": 3599,
    "refresh_token": "OEuVKn7iZ/rJYPi2cNSGZk3NQvWWvD06vnItL0Ptg4s=",
    "scope": "email offline_access openid profile sign"
}
```

3.2 Resource Owner Password Credentials

Thông tin đăng nhập vào hệ thống VNPT SmartCA của người dùng được gửi thông qua ứng dụng phía đối tác.



Được triển khai trong trường hợp tài khoản trên hệ thống VNPT SmartCA được đồng bộ với tài khoản ứng dụng phía đối tác (khác nhau thông tin đăng nhập).

Để sử dụng hình thức phân quyền này, đối tác cần chứng minh được sự an toàn của ứng dụng với VNPT.

Token request:

- URL DEMO: https://rmgateway.vnptit.vn/auth/token
- URL PRODUCTION: https://gwsca.vnpt.vn/auth/token
- HTTP Method: **POST**
- HTTP Content-Type: **x-www-form-urldencoded**
- HTTP Body:

Key	Type	Description
grant_type	String	Yêu cầu giá trị là password
client_id	String	Định danh ứng dụng client
client_secret	String	Chuỗi giá trị bí mật tương ứng với ứng dụng client
username	String	Personal ID đã gửi vào trong email người dùng
password	String	Mật khẩu đăng nhập tài khoản người dùng

- Tất cả tham số trên là bắt buộc.
- Tham số **grant_type** bắt buộc đặt giá trị "**password**".
- Thông tin Client Authentication (**client_id, client_secret**).

Token response:

- HTTP Content-Type: **application/json: charset=utf-8**
- HTTP Body response:

Key	Type	Description
`access_token`	String	Giá trị access_token định dạng JWT
`refresh_token`	String	Giá trị refresh_token dùng để yêu cầu access_token mới khi hết hạn.
`token_type`	String	Định dạng token. Mặc định là `bearer`
`expires_in`	String	Thời gian hiện lực của access_token tính bằng giây
`scope`	String	Thông tin các access mà access token này được cấp

- Mẫu response

```
{
    "access_token": "eyJ0eXAiOiJKV1QiLCJhbGc...",
    "refresh_token": "dV5o7erpj/GCdWAW2zQkcLsiX0bUUYSLGhwa4d7BIKE="
    "token_type": "bearer",
    "expires_in": 3599,
    "refresh_token": "OEuVKn7iZ/rJYPi2cNSGZk3NQvWWvD06vnItL0Ptg4s=",
    "as:client_id": "46ce-636712153955329604.apps.signserviceapi.com",
    "scope": "email offline_access openid profile sign"
```

4 Định nghĩa tham số

4.1 Request

- HTTP Content-Type: `application/json; charset=utf-8`
- HTTP Header: `Authorization : Bearer <access_token>`
- HTTP Body:

Với request yêu cầu account login, bổ sung thêm header property sau:
Key=Authorization
Value=Bearer <access_token>

4.2 Response

- HTTP Content-Type: **application/json: charset=utf-8**
- HTTP Response Body:

Key	Type	Description
ResponseID	String	Chuỗi định danh response dùng để kiểm tra xem có khớp với request không.
ResponseCode	Int	Mã kết quả trả về
ResponseContent	String	Mô tả mã kết quả
Content	object	Dữ liệu trả về cho từ hàm định dạng json object hoặc json array.

- Mẫu response body

```
{
    "ResponseID": "5b483845-35b6-48c9-b9a6-3a4024271271",
    "ResponseCode": 1,
    "ResponseContent": "Success",
    "Content": {
        "Email": "tuanbs@vnpt.vn",
        "PhoneNumber": "0947156062",
        "HoTenDayDu": "Bùi Sĩ Tuấn",
        "GioiTinh": true,
        "DiaChi": "Hà Nội",
        "NgaySinh": "1993-03-21T08:00:00",
        "Group": {
            "ID": "89dc870e-c7e6-4339-a562-1616e4db7b13",
            "AdminEmail": "tuanbs@vnpt.vn",
            "TenNhom": "CThucDT-PM1-eGov",
            "GroupType": 0,
            "SoLuotKyConLai": 253,
            "NgayHetHan": "2020-04-01T00:00:00"
        },
        "Groups": [
            {
                "ID": "89dc870e-c7e6-4339-a562-1616e4db7b13",
                "AdminEmail": "tuanbs@vnpt.vn",
                "TenNhom": "CThucDT-PM1-eGov",
                "GroupType": 0,
                "SoLuotKyConLai": 253,
                "NgayHetHan": "2020-04-01T00:00:00"
            }
        ]
    }
}
```

4.3 Mã trả về thường gặp

Các giá trị thường gặp cho thuộc tính **ResponseCode**

STT	Mã trả về	Ý nghĩa
	1	Success
	53	Two Factor Authentication required for this account
	10000	No account found for input email

	10001	Account is not activated
	10002	Account is locked or deleted
	10003	Second password not set
	10011	OTP is invalid
	11001	No valid service pack for current account
	11002	ServiceGroupID invalid
	11003	ServicePack expired or or signatures count limit exceeded
	12001	Unsupported input file type
	13001	Certificate not found
	13002	Certificate and Account not match
	13003	Certificate expired
	14001	Failed to create signature
	14002	PDF header signature not found
	14003	No signature worker for this account
	15001	Cannot archive signed file
	16001	Transaction information not found
	16002	Transaction file not found
	30000	Request parameter is required
	30001	ServiceID is required
	30002	Unsuported ServiceID
	30003	FunctionName is required
	30004	Unsuported FunctionName
	30005	Account authenticate required
	30006	Account email required
	30010	Invalid input
	31001	ServiceGroupID parameter required
	31002	CertID parameter required
	32001	Token parameter expired
	50000	Service internal error

	50001, 50002, 50003, 50004,	Database protection error
	50005	Send change second pasword failed
	50006	OTP send failed
	51000	Email template file not found

5 Chi tiết API

5.1 User

5.1.1 Userinfo

- Mục đích: Lấy thông tin tài khoản người dùng
- URL DEMO: https://rmgateway.vnptit.vn/identityapi/userinfo/info
- URL PRODUCTION: https://gwsca.vnpt.vn/identityapi/userinfo/info
- Authorize: Bearer token
- Tham số **Paramter**: Không yêu cầu

- Request mẫu

```
{
}
```

- Response Content

Key	Type	Description
accType	int	Loại thuê bao **0: Khách hàng cá nhân** **1: Khách hàng doanh nghiệp** **2: Cá nhân trong doanh nghiệp** **3: Onetime CA**
uidPre	string	Loại giấy tờ (CMND, CCCD, …)
uid	string	Số CMND, CCCD
email	string	Địa chỉ email của thuê bao
phone	string	Số điện thoại của thuê bao

- ResponseCode

Value	Description
1	Success

- Response mẫu


```
{
    "accType": 0,
    "accTypeDesc": "INDIVIDUAL",
    "uidPre": "cmnd",
    "uid": "173844192",
    "email": "tuanbs208@gmail.com",
    "phone": "0947156063",
    "fullName": "Bùi Sĩ Tuấn",
    "gender": 0,
    "address": "Hà Nội",
    "dateOfBirth": "2021-06-10T08:35:35.373Z",
    "status": 2,
    "statusDesc": "ACTIVE"
}
```


5.2 Credential and Signature

5.2.1 List credential

- Mục đích: Lấy danh sách credential của thuê bao.
- URL DEMO: https://rmgateway.vnptit.vn/csc/credentials/list
- URL PRODUCTION : https://gwsca.vnpt.vn/csc/credentials/list
- Authorize: Bearer token
- Tham số **Paramter**: Không yêu cầu

- Request mẫu


```
{
}
```


- Response mẫu

Trả lại danh sách ID credential của thuê bao


```
{
    "code": 0,

    "codeDesc": null,
    "message": null,
    "content": [
        "5d5c0a0f-59b8-498c-9e8e-c3e9b8f1e718"
    ]
}
```

5.2.2 Credential Info

- Mục đích: Lấy thông tin credential của thuê bao (thông tin chứng thư, thông tin khóa ký)
- URL DEMO: https://rmgateway.vnptit.vn/csc/credentials/info
- URL PRODUCTION: https://gwsca.vnpt.vn/csc/credentials/info
- Authorize: Bearer token
- Tham số Paramter:

Key	Type	Description
credentialId	string	*(Required)* ID credential của thuê bao
certificates	string	*(Required)* Kiểu trả về chứng thư số của thuê bao - **none: Không trả về trong kết quả** - **single: Chỉ trả về chứng thư số của thuê bao** - **chain: Trả về danh sách chứng thư bao gồm của thuê bao và của CA**
certInfo	boolean	*(Optional)* Có trả về thông tin chứng thư hoặc không
authInfo	boolean	*(Optional)* Có trả về thông tin kiểu xác thực của thuê bao hoặc không

- Request mẫu

```
{
    "credentialId": "5d5c0a0f-59b8-498c-9e8e-c3e9b8f1e718",
    "certificates": "chain",
    "certInfo": true,
    "authInfo": true
}
```

- Response mẫu

```
{
    "cert": {
        "status": "VALID",
        "serialNumber": "54010101f7c06634fd6fd5d3a93b340f",
        "subjectDN": "C=VN,ST=HẢI PHÒNG,L=Quận,CN=VNPT Test HueNTN,UID=CMND:013419012",
        "issuerDN": "CN=VNPT Certification Authority TEST,O=VNPT,C=VN",
        "certificates": [

"MIIEGTCCA4KgAwIBAgIQVAEBAffAZjT9b9XTqTs0DzANBgkqhkiG9w0BAQUFADBIMSowKAYDVQQDDCFWTlBUIEN
lcnRpZmljYXRpb24gQXV0aG9yaXR5IFRFU1QxDTALBgNVBAoMBFZOUFQxCzAJBgNVBAYTAlZOMB4XDTIxMDgxNjA
1MDYwMFoXDTIyMDgxNjE3MDYwMFowcDELMAkGA1UEBhMCVk4xFTATBgNVBAgMDEjhuqJJIFBIw5JORzEPMA0GA1U
EBwwGUXXhuq1uMRkwFwYDVQQDDBBWTlBUIFRlc3QgSHVlTlROMR4wHAYKCZImiZPyLGQBAQwOQ01ORDowMTM0MTk
wMTIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCrAbzlnODzb555Pamh2gwk+6Fg8yU13aoFu4ERsMd
dM6piWe99xYfuhQe8kRa32TwotQ8G0QtJBbjwlI91scXpdLjrFlebRoaEeyGTJ7ge5tHl+7m7F/iED90YhabrPBv
kdcwLgCW2u+/wA2aiceouYKTYu6eRUkGgS49D3tqSn3S4GqtshC9KevwojPxY0UbrvTHqZk/ZrwrAhssrptIVqCX
4otyMtVfaw/LhrA0y/SHkjXjeHzWMFh4/v0N0zcyrzqH+mUvf9XjI631QiqMjfR92VMogTVaJ2vCeaDfeC0cPIzY
J6hcc+NNoRJlMUp/uc2k1D2WXSLFQcL3psnDnAgMBAAGjggFWMIIBUjBCBggrBgEFBQcBAQQ2MDQwMgYIKwYBBQU
HMAKGJmh0dHA6Ly9wdWIudm5wdC1jYS52bi9jZXJ0cy92bnB0Y2EuY2VyMB0GA1UdDgQWBBRW28Xakj1l5xOIYfU
FVZy2lkUzuTAMBgNVHRMBAf8EAjAAMB8GA1UdIwQYMBaAFOyVxCbDabShO3LsrefXzzaJxQpzMGgGA1UdIARhMF8
wXQYOKwYBBAGB7QMBAQMBBAMwSzAiBggrBgEFBQcCAjAWHhQAUABJAEQALQBQAFIALQAxAC4AMDAlBggrBgEFBQc
CARYZaHR0cDovL3B1Yi52bnB0LWNhLnZuL3JwYTAOBgNVHQ8BAf8EBAMCBPAwKQYDVR0lBCIwIAYIKwYBBQUHAwI
GCCsGAQUFBwMEBgorBgEEAYI3CgMMMBkGA1UdEQQSMBCBDm50bmh1ZUB2bnB0LnZuMA0GCSqGSIb3DQEBBQUAA4G
BAFGWJt48Dh86MDyoWWNaOwgdU3qwTsj6PSyIQJ3joCuCOO8vkmzgy/8XZ8ciYM6CSheMatjz780vetXp/jOcyPB
bZt3sayqR9EiqNh+ar9BnzETXhth4q4XgTTU5i3jU8h0CAoUQBUPWNpj4oUqeu8aALE0GvFwn3JaPIYR0xQHn\r\
n",

"MIICeDCCAeGgAwIBAgIQVAEBAd94ePRfzYWgXXvdITANBgkqhkiG9w0BAQUFADBIMSowKAYDVQQDDCFWTlBUIEN
```

```
lcnRpZmljYXRpb24gQXV0aG9yaXR5IFRFU1QxDTALBgNVBAoMBFZOUFQxCzAJBgNVBAYTAlZOMB4XDTIwMDcyNzA
4NTgxN1oXDTI1MDcyNzA4NTgxN1owSDEqMCgGA1UEAwwhVk5QVCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSBURVN
UMQ0wCwYDVQQKDARWTlBUMQswCQYDVQQGEwJWTjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAhB+aPz+WH53
6Jlf0fziJPDcpMRVGlJpxtOnRSrP5OOtloo9kNs1wNihs777d10LUjVoMCe37mYNrtJfqEn2dBJlCkTVDeMY4MKi
jOMqox3NbrWKbGFO+a/LyZ5tgn0hYCOOnLi0+yCD9HH1+YB8KXBcJebwqZp0+/0SaoXfZ+lMCAwEAAaNjMGEwHQY
DVR0OBBYEFOyVxCbDabShO3LsrefXzzaJxQpzMA8GA1UdEwEB/wQFMAMBAf8wHwYDVR0jBBgwFoAU7JXEJsNptKE
7cuyt59fPNonFCnMwDgYDVR0PAQH/BAQDAgGGMA0GCSqGSIb3DQEBBQUAA4GBAG5nWPw+ARlS/0kCwfBFZ3QRcZa
bOO7Mr9LSBThfUnndhcWUwngMmGY1Oew74qXkIT7KofKyNpSeGPvYJRAIgIjE7bNOhPzLGAJGZ8VTOI72UbN4FPZ
cse11RJrTL02bn61G61wLzeN6H0MXm2Wo/eNOBWF95AsiTryN3wlD5zzJ\r\n"
        ],
        "validFrom": "20210816050600Z",
        "validTo": "20220816050600Z"
    },
    "key": {
        "status": "ENABLED",
        "alg": [
            "1.2.840.113549.1.1.1"
        ],
        "len": 2048
    },
    "authMode": "oauth2code",
    "scal": "SCAL2",
    "multisign": 1,
    "status": "VALID"
}
```


5.2.3 Sign

- Mục đích: Gửi yêu cầu ký hash. Sau khi gửi yêu cầu thành công, thuê bao sẽ nhận được notification trên mobile app. Hệ thống phía đối tác sử dụng api get transaction info để kiểm tra trạng thái của giao dịch.
- URL DEMO: https://rmgateway.vnptit.vn/csc/signature/sign
- URL PRODUCTION: https://gwsca.vnpt.vn/csc/signature/sign
- Tham số **Paramter**:

Key	Type	Description
credentialId	string	*(Required)* ID credential của thuê bao
refTranId	string	*(Optional)* ID giao dịch phía đối tác
notifyUrl	string	*(Optional)* Sau khi thuê bao xác nhận giao dịch ký số, SmartCA sẽ gọi URL này 01 lần duy nhất ở server side to server side. Đối tác cần build URL này để nhận kết quả từ SmartCA (HTTP POST). Dữ liệu định dạng **application/json**: `{ tranId = (string)"ID giao dịch ký số của SmartCA", refTranId = (string)<ID giao dịch phía đối tác>, status = (byte)<Trạng thái giao dịch ký số> }`
description	string	*(Optional)* Mô tả thông tin giao dịch
datas	List	*(Required)* Danh sách file yêu cầu ký số **(tối đa 10)**

- Request mẫu

```
{
    "credentialId": "5d5c0a0f-59b8-498c-9e8e-c3e9b8f1e718",
```

```
    "refTranId": "e442f592-f892-43dd-8a4b-d6339679f27f",
    "notifyUrl": https://localhost/kyso/callback,
    "description": "Pdf sign file sample",
    "datas": [
        {
            "name": "sample.pdf",
            "dataBase64": " JVBERi0xLjUNCiW1tbW1DQoxIDAgb2JqDQo8PC9UeXBlL0NhdGFs…"
        }
    ]
}
```

- ResponseCode

Value	Description
1	Success

- Response mẫu

```
{
    "code": 0,
    "codeDesc": "SUCCESS",
    "message": "Chờ người dùng xác nhận",
    "content": {
        "tranId": "1e516e32-5091-4cf2-be36-e002cf08e013"
    }
}
```

5.2.4 Sign hash

- Mục đích: Gửi yêu cầu ký hash. Sau khi gửi yêu cầu thành công, thuê bao sẽ nhận được notification trên mobile app. Hệ thống phía đối tác sử dụng api get transaction info để kiểm tra trạng thái của giao dịch.
- URL DEMO: https://rmgateway.vnptit.vn/csc/signature/signhash
- URL PRODUCTION: https://gwsca.vnpt.vn/csc/signature/signhash
- Authorize: Bearer token
- Tham số **Paramter**:

Key	Type	Description
credentialId	string	*(Required)* ID credential của thuê bao
refTranId	string	*(Required)* ID giao dịch phía đối tác
notifyUrl	string	*(Optional)* Sau khi thuê bao xác nhận giao dịch ký số, SmartCA sẽ gọi URL này 01 lần duy nhất ở server side to server side. Đối tác cần build URL này để nhận kết quả từ SmartCA (HTTP POST). Dữ liệu định dạng **application/json**: `{ tranId = (string)"ID giao dịch ký số của SmartCA", refTranId = (string)<ID giao dịch phía đối tác>, status = (byte)<Trạng thái giao dịch ký số> }`
description	string	*(Optional)* Mô tả thông tin giao dịch

datas	List	*(Required)* Danh sách hash yêu cầu ký số **(tối đa 50)**

- Request mẫu

```
{
    "credentialId": "5d5c0a0f-59b8-498c-9e8e-c3e9b8f1e718",
    "refTranId": "e442f592-f892-43dd-8a4b-d6339679f27f",
    "notifyUrl": "https://localhost/kyso/callback",
    "description": "Pdf signhash sample",
    "datas": [
        {
            "name": "sample.pdf",
            "hash": "y4ahlQA4RZxb1Fh7V6dfK84ga3nnEecSdroDx1LmLGE="
        },
        {
            "name": "sample.docx",
            "hash": "W3siRGF0YSI6ICI3QTRiamJPU3dCTEVyS0ZHdlRvZTI2T0ZTR2M9In1d"
        }
    ]
}
```

- ResponseCode

Value	Description
1	Success

- Response mẫu

```
{
    "code": 0,
    "codeDesc": "SUCCESS",
    "message": "Chờ người dùng xác nhận",
    "content": {
        "tranId": "1e516e32-5091-4cf2-be36-e002cf08e013"
    }
}
```

5.2.5 Get Transaction Info

- Mục đích: Kiểm tra trạng thái giao dịch trong khi chờ thuê bao xác nhận trên mobile app.
- URL DEMO: https://rmgateway.vnptit.vn/csc/credentials/gettraninfo
- URL PRODUCTION: https://gwsca.vnpt.vn/csc/credentials/gettraninfo
- Authorize: Bearer token
- Tham số **Paramter**:

Key	Type	Description
tranId	String	*(Required)* ID giao dịch trả về từ api signhash

- Request mẫu

```
{
    "tranId": "1e516e32-5091-4cf2-be36-e002cf08e013"

}
```

- ResponseCode

Value	Description
0	Success.

- Response mẫu

```
{
    "code": 0,
    "codeDesc": "SUCCESS",
    "message": "success",
    "content": {
        "refTranId": "e442f592-f892-43dd-8a4b-d6339679f27f",
        "documents": [
            {
                "name": "sample.pdf",
                "type": "pdf",
                "size": "30KB",
                "data": "y4ahlQA4RZxb1Fh7V6dfK84ga3nnEecSdroDx1LmLGE=",
                "hash": "y4ahlQA4RZxb1Fh7V6dfK84ga3nnEecSdroDx1LmLGE=",
                "sig": null,
                "dataSigned": null,
                "url": null
            },
            {
                "name": "sample.pdf",
                "type": "pdf",
                "size": "30KB",
                "data": "y4ahlQA4RZxb1Fh7V6dfK84ga3nnEecSdroDx1LmLGE=",
                "hash": "y4ahlQA4RZxb1Fh7V6dfK84ga3nnEecSdroDx1LmLGE=",
                "sig": null,
                "dataSigned": null,
                "url": null
            }
        ],
        "tranId": "1e516e32-5091-4cf2-be36-e002cf08e013",
        "sub": "879f198d-bce0-4617-892f-c6c7a8c79fb7",
        "credentialId": "5d5c0a0f-59b8-498c-9e8e-c3e9b8f1e718",
        "tranType": 3,
        "tranTypeDesc": "SIGNHASH",
        "tranStatus": 4000,
        "tranStatusDesc": "WAITING_FOR_SIGNER_CONFIRM",
        "reqTime": "2021-08-22T10:18:34.87Z"
    }
}
```

Trạng thái của Transaction được mô tả (tranStatusDesc = tranStatus) như sau:

SUCCESS = 1,

WAITING_FOR_SIGNER_CONFIRM = 4000,

EXPIRED = 4001,

SIGNER_REJECTED = 4002,

AUTHORIZE_KEY_FAILED = 4003,

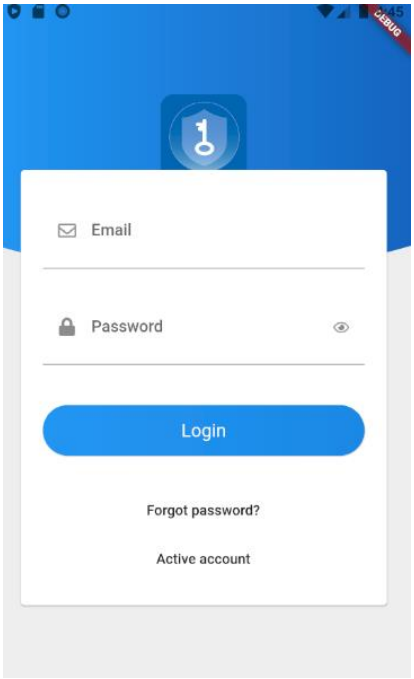
SIGN_FAILED = 4004

6 Xác nhận giao dịch trên app mobile

6.1. Kích hoạt tài khoản thuê bao

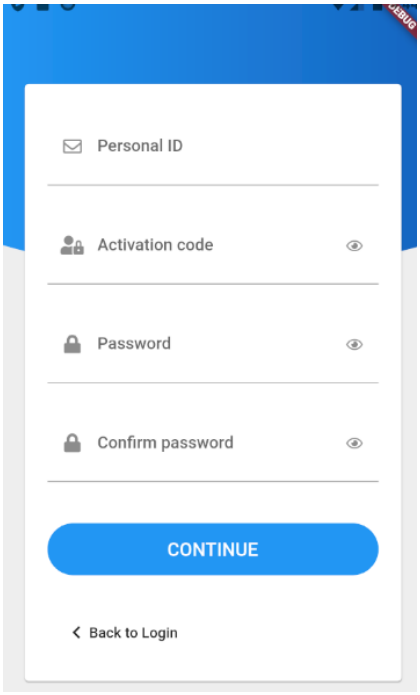
Để thực hiện kích hoạt tài khoản

- Bước 1: Mở ứng dụng VNPT-Smart CA
- Bước 2: Chọn 'Active account' ở màn hình đăng nhập



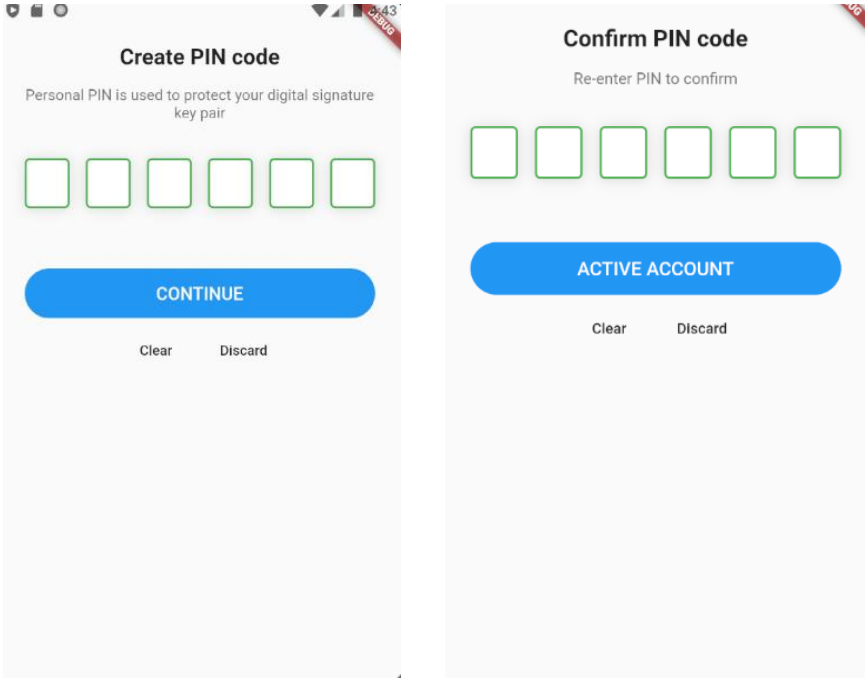
Hình 1: Giao diện đăng nhập

- Bước 3: Điền thông tin tài khoản bao gồm : CCCD, mã kích hoạt, mật khẩu, xác nhận mật khẩu



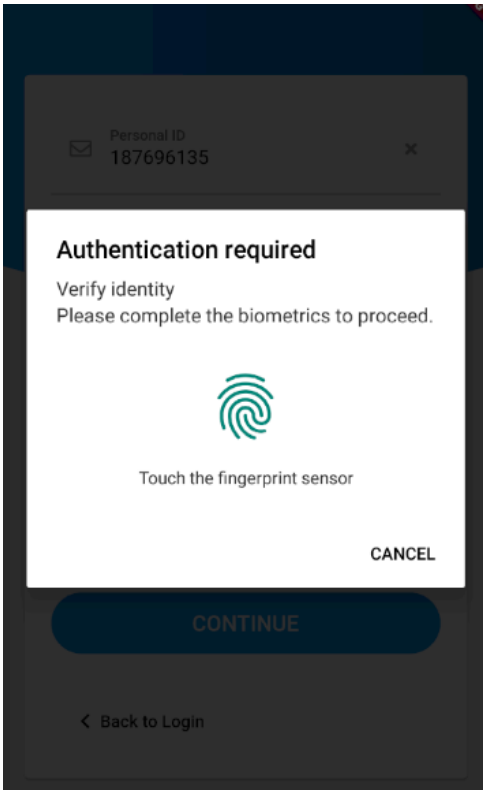
Hình 2: Giao diện nhập thông tin tài khoản

- Bước 4: Khởi tạo và xác nhận mã PIN cá nhân



Hình 3: Giao diện khởi tạo mã PIN

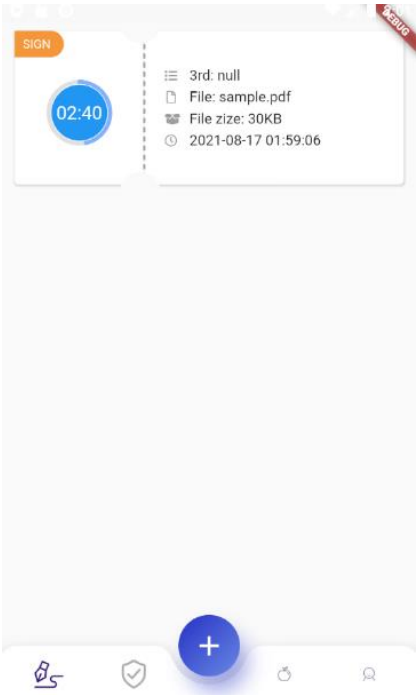
- Bước 6: Kích hoạt xác thực sinh trắc học



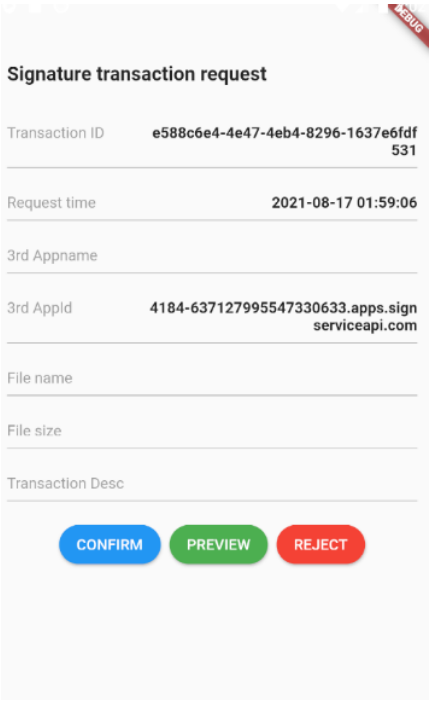
Hình 4: Giao diện kích hoạt xác thực sinh trắc học

6.2. Xác nhận giao dịch ký số

- Bước 1: Người dùng khởi tạo giao dịch ký số trên hệ thống (hệ thống đối tác như: hệ thống eOffice, eContract, hệ thống ngân hàng, chứng khoán)
- Bước 2: Người dùng mở app VNPT SmartCA tiến hành đăng nhập tài khoản
- Bước 3: Người dùng bấm chọn giao dịch cần xác nhận ở mục ký số

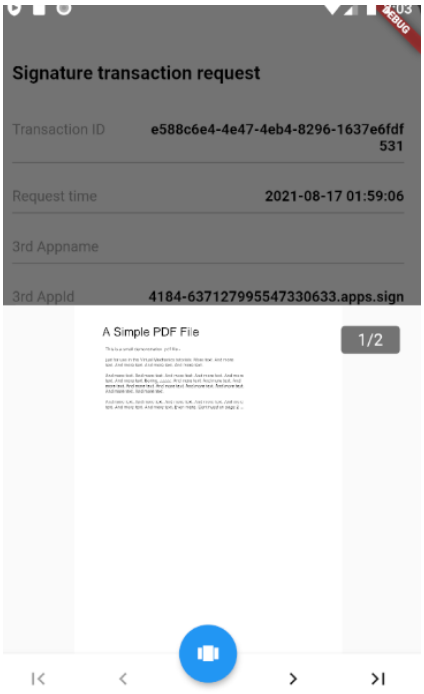


Hình 6: Giao diện mục ký số



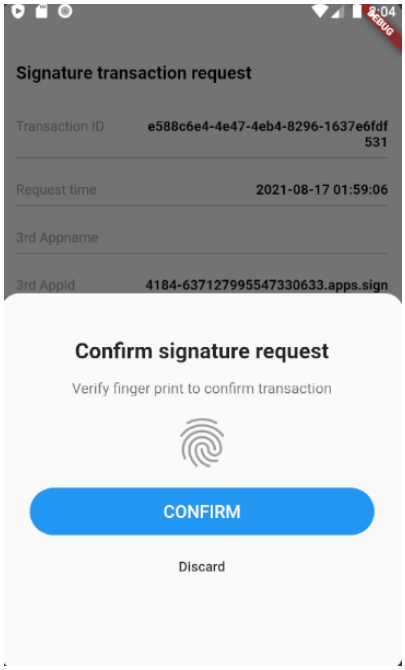
Hình 7: Giao diện thông tin giao dịch

- Bước 4 (không bắt buộc): Đối với giao dịch ký file pdf, người dùng chọn 'PREVIEW' để xem lại file pdf cần ký



Hình 8: Giao diện preview pdf

- Bước 5: Chọn 'CONFIRM' để xác nhận hoàn tất giao dịch, chọn 'CANCLE' để xác nhận hủy giao dịch
- Bước 6: Hoàn tất xác thực (sinh trắc học hoặc mã PIN) để kết thúc giao dịch



Hình 9: Hoàn tất giao dịch bằng xác thực sinh trắc học

7 Code mẫu tích hợp

https://drive.google.com/drive/folders/15XKfk_PV4eiLpa4xvZlV2EnSEBBfIsV0?usp=sharing