BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 936 /BTTTT-NEAC V/v hướng dẫn tích hợp tính năng ký số vào cổng dịch vụ công	*Hà Nội, ngày 22 tháng 3 năm 2023*

Kính gửi:

- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương.

Thực hiện chỉ đạo của Thủ tướng Chính phủ tại Chỉ thị số 05/CT-TTg ngày 23/02/2023 về Tiếp tục đẩy mạnh triển khai đề án phát triển ứng dụng dữ liệu về dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022 - 2025, tầm nhìn đến năm 2030 tại các bộ, ngành, địa phương năm 2023 và những năm tiếp theo, Bộ Thông tin và Truyền thông (TT&TT) đã xây dựng Hướng dẫn tích hợp tính năng ký số từ xa (chữ ký số trên thiết bị di động thông minh) để thuận tiện cho các đơn vị vận hành cổng dịch vụ công (DVC) trong quá trình tích hợp chữ ký số công cộng theo mô hình ký số từ xa vào các tác vụ của người dân/doanh nghiệp trên cổng *(Phụ lục đính kèm theo Công văn này)*.

Ngoài ra, để thuận lợi hơn trong công tác tích hợp, Bộ TT&TT cũng đã chuẩn bị bảng khảo sát, đánh giá tính sẵn sàng của hệ thống kỹ thuật trong quá trình tích hợp tính năng ký số nói chung và ký số từ xa nói riêng, trân trọng đề nghị Quý đơn vị điền thông tin và gửi về Bộ TT&TT (qua Trung tâm Chứng thực điện tử quốc gia) theo địa chỉ: Tầng 7, 115 Trần Duy Hưng, Phường Trung Hòa, Quận Cầu Giấy, Thành phố Hà Nội; bản mềm gửi vào thư điện tử: lnhan@mic.gov.vn **trước ngày 10/04/2023**.

Trong quá trình triển khai, nếu Quý đơn vị gặp khó khăn vướng mắc hoặc phát sinh vấn đề cần trao đổi, làm rõ, đề nghị liên hệ theo đầu mối: Ông Lê Nam Hàn, Trung tâm Chứng thực điện tử quốc gia, điện thoại: 0963124659, thư điện tử: lnhan@mic.gov.vn.

Trân trọng cảm ơn./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng;
- Các cục: ATTT, CĐSQG (để p/h);
- Các Sở TT&TT (để p/h);
- Lưu: VT, NEAC.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Huy Dũng

PHIẾU KHẢO SÁT HIỆN TRẠNG KỸ THUẬT CỦA CỔNG DỊCH VỤ CÔNG

STT	Thông tin	Mô tả
1	Tên cổng dịch vụ công	
2	Địa chỉ trang web	
3	Hệ điều hành máy chủ (Windows Server, CentOS, Ubuntu, RHEL...)	
4	Nền tảng lập trình (.NET framework, .Net Core, JVM)	
5	Ngôn ngữ lập trình (Java, C#, Python, PHP...)	
6	Loại tệp cần ký (PDF, XML, JSON)	
7	Đầu mối liên hệ	Điện thoại: Email: Tên: Chức danh:
8	Công ty/tổ chức chịu trách nhiệm các vấn đề liên quan đến kỹ thuật	Tên: Địa chỉ:

Đầu mối liên hệ: Ông Lê Nam Hàn, Trung tâm Chứng thực điện tử quốc gia, điện thoại: 0963124659, thư điện tử: lnhan@mic.gov.vn.

Bản mềm của phiếu khảo sát có tại địa chỉ: https://neac.gov.vn/vi/tin-tuc-su-kien/detail/khao-sat-so-lieu/phieu-khao-sat-hien-trang-ky-thuat-cua-cong-dich-vu-cong-312.htm

PHỤ LỤC

(Ban hành kèm theo công văn số 956 /BTTTT-NEAC ngày 22 tháng 5 năm 2023 của Bộ Thông tin và Truyền thông)

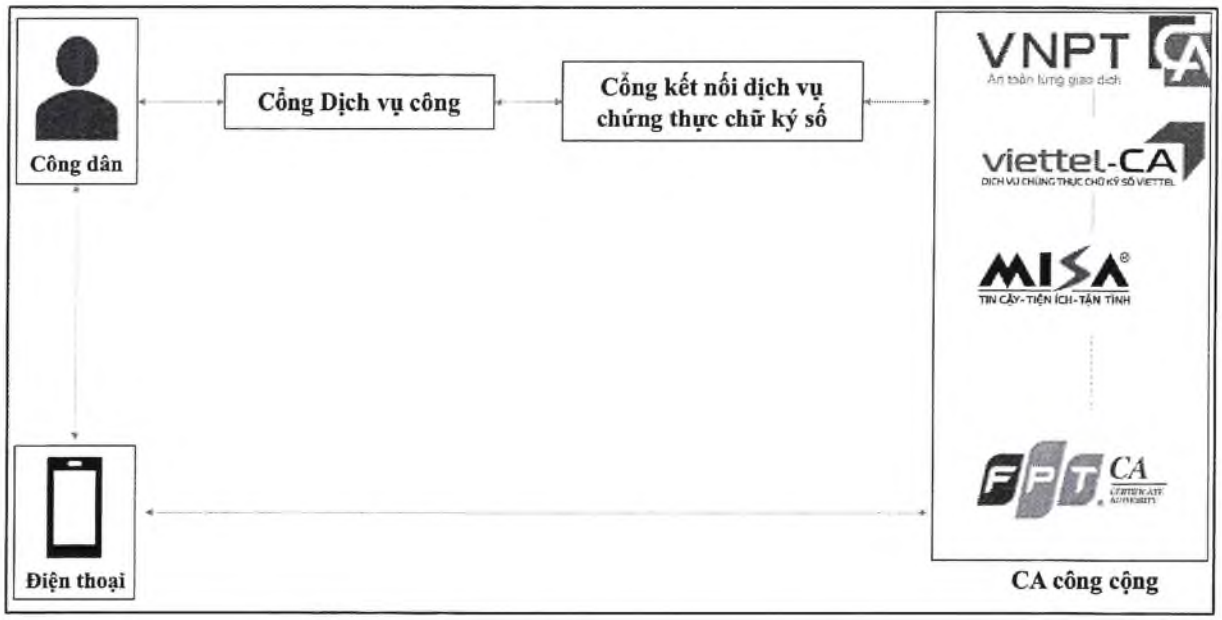
HƯỚNG DẪN KẾT NỐI CỔNG DỊCH VỤ CÔNG VỚI CỔNG KẾT NỐI DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG

(Phiên bản 1.1)

Mục lục

I. MÔ HÌNH TỔNG QUAN

Mô hình kết nối giữa Cổng kết nối dịch vụ chứng thực chữ ký số công cộng (sau đây gọi là Cổng eSign) (theo khoản 12 Điều 3 Nghị định 42/2022/NĐ-CP), cổng dịch vụ công (sau đây gọi là Cổng DVC) và các Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng (sau đây gọi là CA công cộng) được mô tả tại sơ đồ như sau:

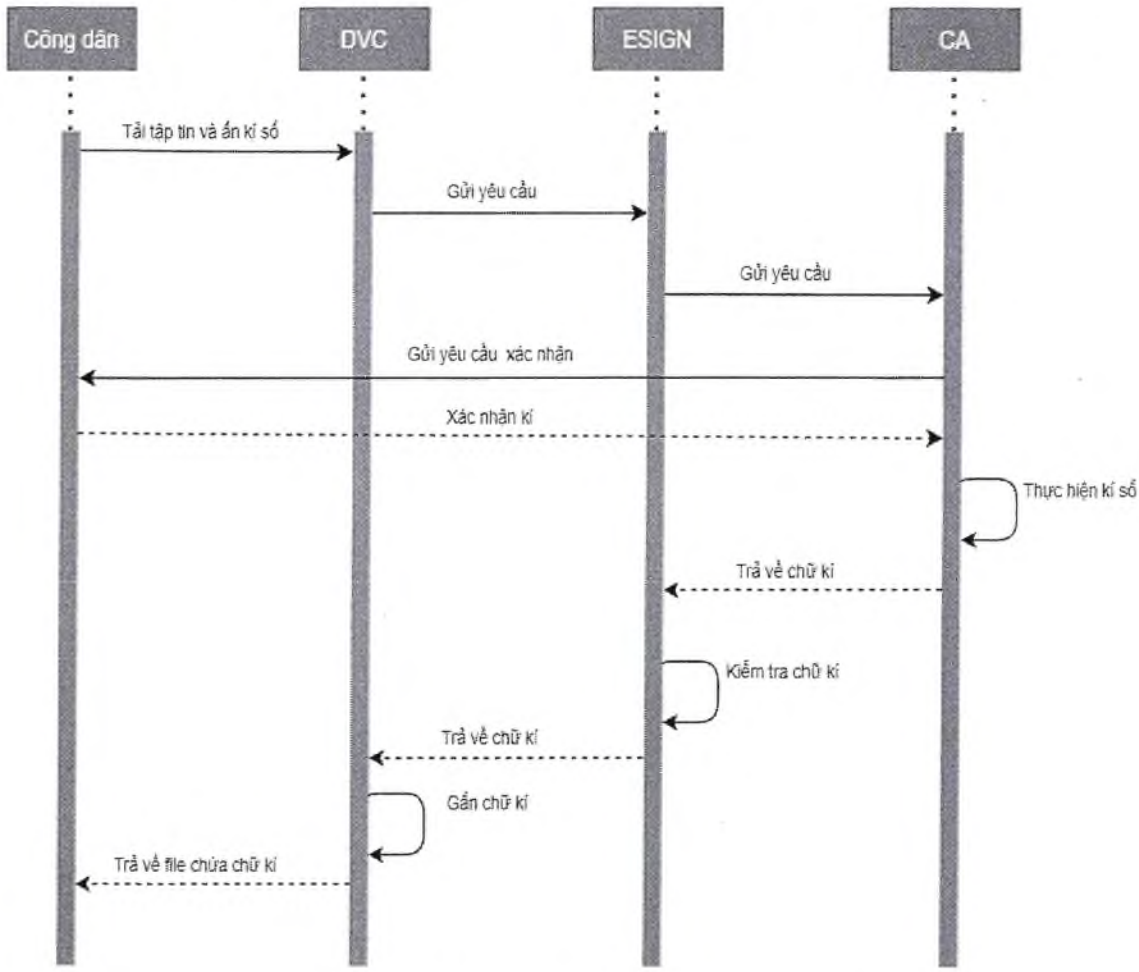


Hình 1 Mô hình kết nối ký số từ xa trên Cổng DVC

Để công dân thực hiện ký số khi tham gia thủ tục hành chính, công dân (người dùng của cổng DVC) cần có chữ ký số (có thể đăng ký ở các CA công cộng). Cổng DVC sau đó chỉ cần kết nối với Cổng eSign, Cổng eSign sẽ gửi yêu cầu ký đến CA công cộng mà công dân là thuê bao. CA công cộng tương ứng sẽ xác thực ký với công dân theo hệ thống cung cấp dịch vụ riêng.

Sau khi đã xác thực và kích hoạt ký, CA công cộng sẽ trả kết quả ký về cho Cổng eSign, Cổng eSign sẽ kiểm tra chữ ký và trả kết quả cho Cổng DVC. Đối với công dân tham gia Cổng DVC, giao diện duy nhất là giao diện của Cổng DVC.

Sơ đồ luồng thực hiện ký số từ xa trên Cổng DVC

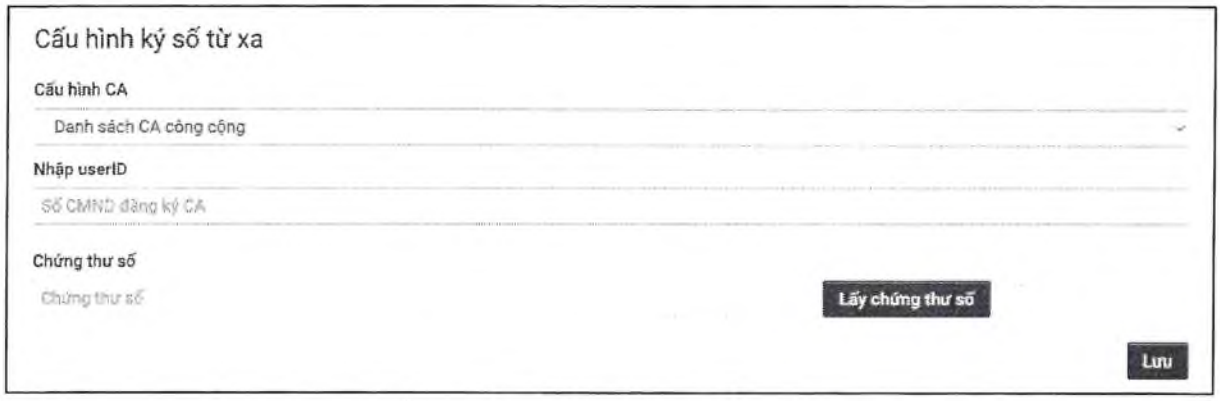


Hình 2 Sơ đồ luồng thực hiện ký số từ xa trên Cổng DVC

1. Công dân tải tập tin cần ký và ấn ký số
2. Cổng DVC gửi yêu cầu ký số và tập tin cần ký đã được băm cho Cổng eSign
3. Cổng eSign gửi yêu cầu ký số và tập tin cần ký cho CA công cộng
4. CA công cộng gửi yêu cầu xác nhận ký số cho công dân qua ứng dụng di động
5. Công dân xác nhận yêu cầu ký số qua ứng dụng di động
6. CA công cộng thực hiện ký số và trả về chữ ký dưới dạng Base64 cho Cổng eSign
7. Cổng eSign tiến hành kiểm tra chữ ký nhận được từ CA công cộng
8. Cổng eSign trả về chữ ký dạng Base64 cho Cổng DVC
9. Cổng DVC gắn chữ ký vào file

II. THIẾT LẬP CẤU HÌNH KÝ SỐ

Cấu hình ký số sẽ được thiết lập trong trang Thông tin cá nhân của Cổng dịch công như sau:



Hình 3 Giao diện cấu hình ký số

Khi thực hiện ký số lên tập tin PDF theo phương thức ký số từ xa, người dùng cần có tài khoản trên Cổng Dịch vụ công và cung cấp các thông tin qua các bước sau:

1. Người dùng chọn CA công cộng mà mình đang là thuê bao từ danh sách dropdown "Chọn CA".

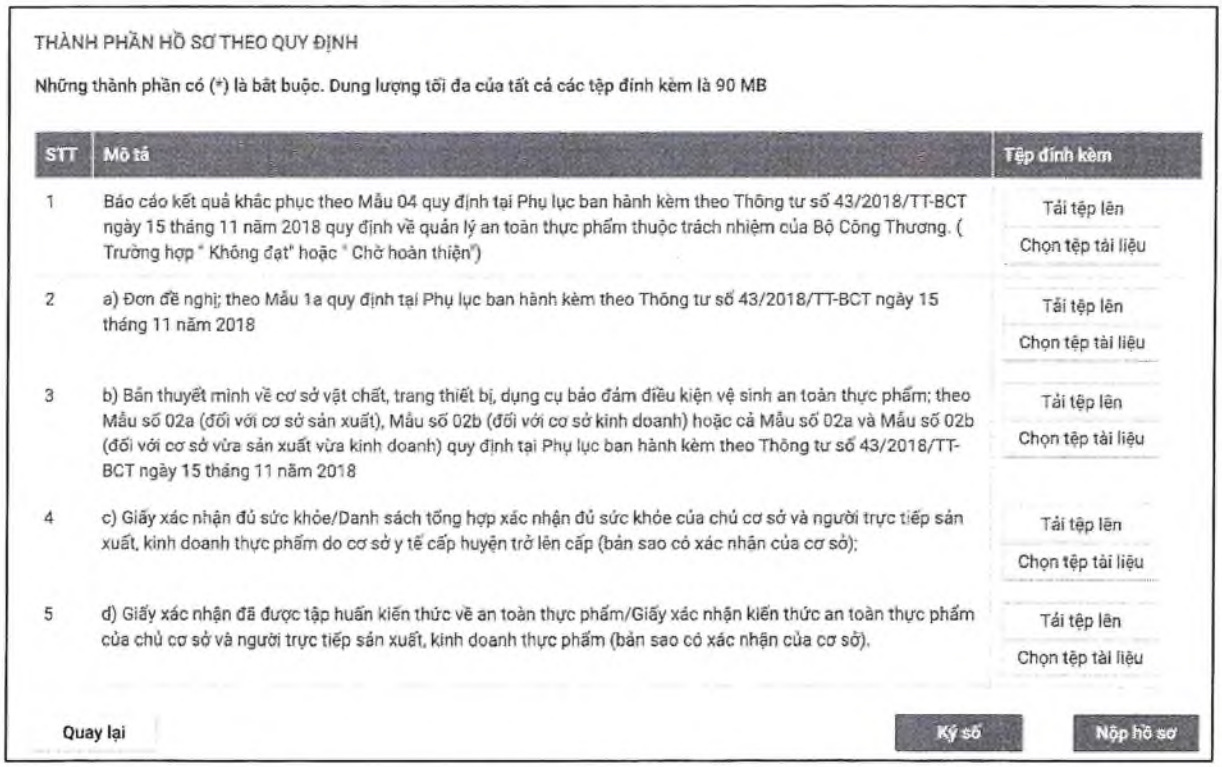
2. Người dùng nhập số CMND hoặc số CCCD đã khai báo khi đăng ký với CA công cộng vào phần "Nhập userID".

3. Nhấn nút "Lấy Chứng thư số". Cổng Dịch vụ công lấy Chứng thư số theo API lấy danh sách chứng thư số.

4. Nhấn Lưu.

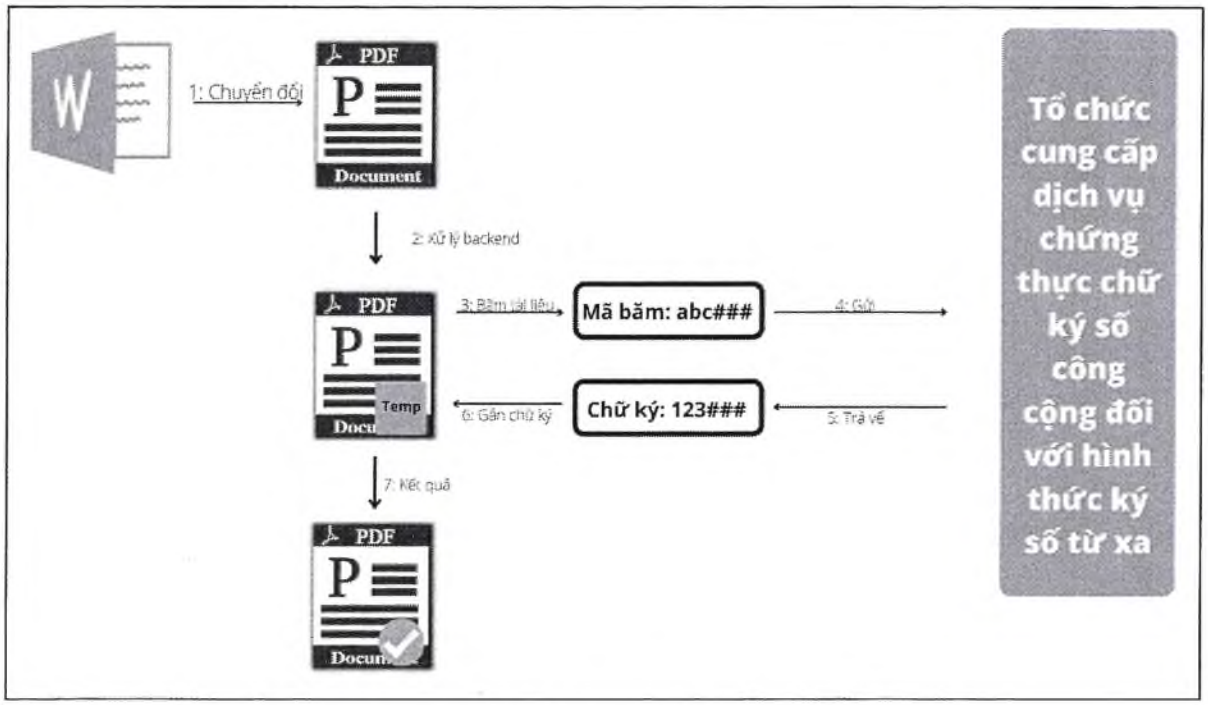
III. QUY TRÌNH KÝ TẬP TIN PDF Ở CỔNG DVC

Sau khi đã cấu hình ký số thành công cho tài khoản, đối với mỗi tài liệu cần ký, người dùng có thể nhấn vào nút ký như sau:



Hình 4 Giao diện ký số tài liệu

Sau khi người dùng nhấn vào nút ký, hệ thống backend cổng Dịch vụ công sẽ thực hiện thông qua sơ đồ sau:



Hình 5 Quy trình ký số từ tập tin PDF phía Cổng DVC

Bước 1: Chuyển tài liệu cần ký thành tập tin PDF (trong trường hợp tài liệu đó không phải là dạng PDF).

Bước 2: Cổng DVC tạo ra tập tin PDF Temp.

Bước 3: Cổng DVC thực hiện băm tập tin.

Bước 4: Cổng DVC gửi mã băm và các thông tin cần thiết theo API đến máy chủ của CA.

Bước 5: Server CA trả về giá trị chữ ký.

Bước 6: Cổng Dịch vụ công gắn chữ ký.

Bước 7: Cổng Dịch vụ trả tập tin đã ký cho người dùng.

IV. CẤU HÌNH HỆ THỐNG KHUYẾN NGHỊ

	Cấu hình tối thiểu	Cấu hình đề nghị
Hệ điều hành	Windows 2008/Ubuntu 16	Windows 2016/Ubuntu20
Nền tảng lập trình	.NET Core/.NET framework 4/Java 1.5	.NET Core/.NET framework 4.8/ Java 8
Ngôn ngữ lập trình	PHP, Python, Java, C#	Java, C#
Loại tệp	PDF, XML, JSON	

V. MÔ TẢ API

1. Thông tin kết nối chung

URL: https://esign.neac.gov.vn/sign_v2

Các dịch vụ cung cấp:

TT	Dịch vụ	API	Mô tả
1	Danh mục chứng thư số của người ký	get_certificate	Phương thức lấy chứng thư số của người sử dụng
2	Ký tài liệu	sign	Ký tập tin được người sử dụng tải lên hệ thống cổng dịch vụ công
3	Kiểm tra trạng thái giao dịch	get_status	Gói tin lấy trạng thái kết quả ký số của người dân

Yêu cầu kỹ thuật

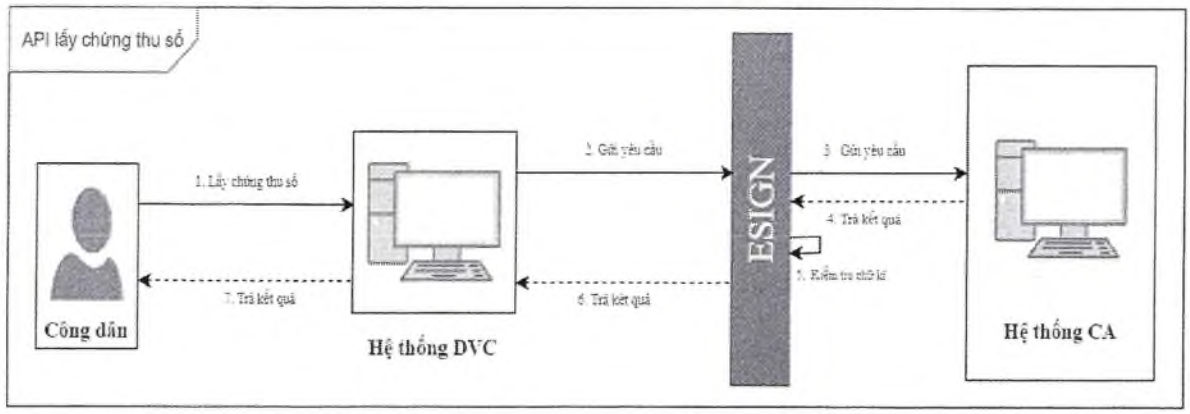
STT	Nội dung	Yêu cầu kỹ thuật
1	sp_credentials	Theo RFC 8265
2	mã băm (hash)	Theo RFC 6234 Chuẩn an toàn hàm băm trong ký số từ xa được quy định trong Thông tư 16/2019/TT-BTTTT và khuyến nghị áp dụng chuẩn hàm băm về ứng dụng CNTT trong cơ quan nhà nước được quy định trong Thông tư 39/2017/TT-BTTTT
3	ký số	Theo Thông tư số 22/2020 của Bộ Thông tin và Truyền thông Quy định về yêu cầu kỹ thuật đối với phần mềm ký số, phần mềm kiểm tra chữ ký số
4	TLS	Theo RFC 8446 Bắt buộc áp dụng an toàn tầng giao vận TLS v1.2 theo Thông tư 39/2017/TT-BTTTT
5	hex	Theo RFC 4648
6	chứng thư số của người dùng	Theo RFC 5280

Bảng mã trạng thái

STT	Status_code	Chú thích
1	200	Thành công
2	400	Tài liệu không hợp lệ
3	401	Credentials không hợp lệ
4	402	Mã hash không đúng định dạng
5	403	Chứng thư bị thu hồi hoặc không rõ định dạng

6	405	Đăng nhập thất bại
7	500	Lỗi hệ thống
8	501	Ký số thất bại

2. API lấy danh sách chứng thư của người dùng



a. Phương thức: POST

b. Đường dẫn: https://esign.neac.gov.vn/sign_v2/get_certificate

c. Đặc tả:

- Tham số đầu vào:

TT	Tham số	Kiểu dữ liệu	Bắt buộc	Chú thích
1	sp_id	string	☑	Username do Cổng eSign cung cấp cho Cổng DVC
2	sp_password	string	☑	Password do Cổng eSign cung cấp cho Cổng DVC
3	user_id	string	☑	Số CCCD/CMND/Hộ chiếu/Mã số thuế/ của cá nhân/tổ chức muốn đăng nhập
4	ca_name	string	☑	Tên của CA công cộng mà Cổng DVC muốn kết nối. (Tham chiếu tên tại url: https://neac.gov.vn/vi/ca-cong-cong/)

- Ví dụ tham số đầu vào:

```
{
    "sp_id": ".....",
    "sp_password": ".....",
    "user_id": ".....",
    "ca_name": ".....",
    "serial_number": "....."
}
```

- Tham số đầu ra:

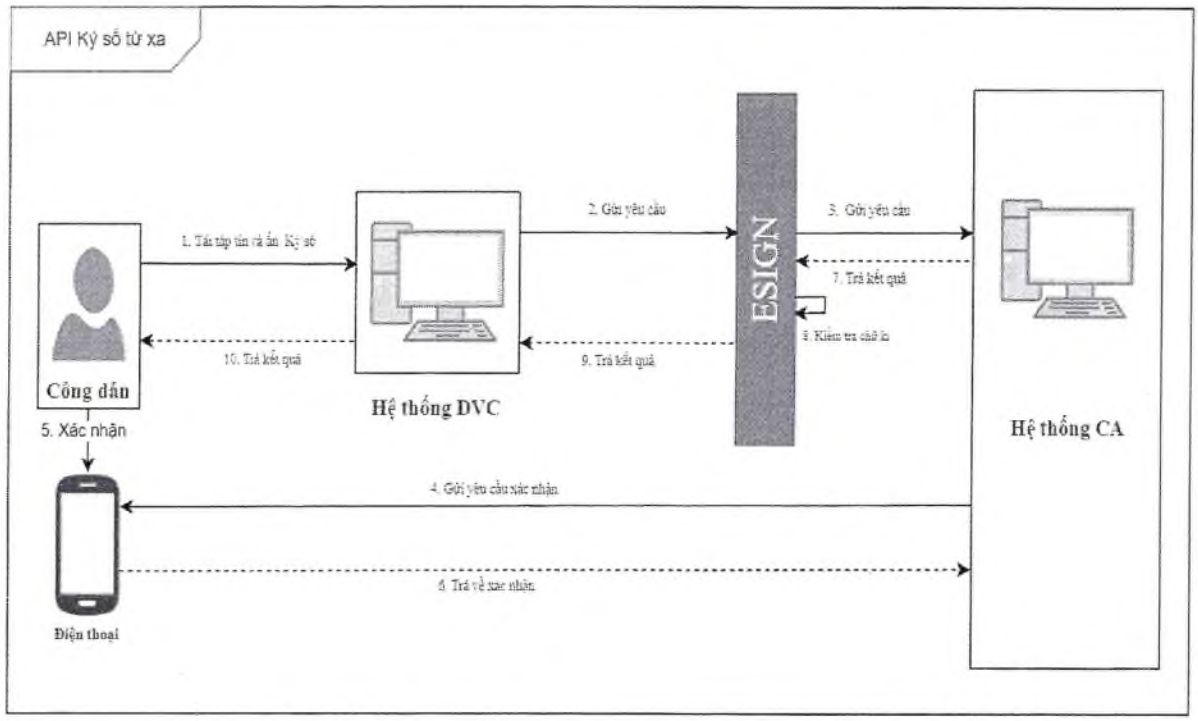
TT	Tham số	Kiểu dữ liệu	Chú thích
1	status_code	int	Mã request thành công hoặc mã lỗi tương ứng. VD: 200, 401, 403, 500…
2	message	string	Thông điệp thành công hoặc thông điệp lỗi tương ứng với mã trạng thái ở status_code.
3	cert_id	string	Định danh chứng thư số (còn gọi là cert alias)
4	cert_data	string	Dữ liệu chứng thư số (dạng base64)
5	chain_data	list<string>	Danh sách chứng thư, gồm 3 phần tử. Phần tử đầu tiên là chứng thư ký, thứ hai là CA, cuối cùng là Root CA do NEAC quản lý.
6	serial_number	String	Số xê-ri của chứng thư số
7	transaction_id	String	Mã định danh giao dịch khởi tạo bởi Cổng eSign

- Ví dụ tham số đầu ra:

```
{
    "status_code": 200,
    "message": "Success",
    "data":
    {
        "transaction_id": "SP_CA_12345",
```

```
            "user_certificates":
            [
                  {
                        "cert_id": "……..",
                        "cert_data":
"MIIGUDCCBTigAwIBAg",
                        "chain_data": {
                              "ca_cert":
"MIIAHDFKBTkeKwIBAu",
                              "root_cert":
"MIIAAJFNCTuwUoPlat"
                        },
                        "serial_number":
"2015000100057d90"
                  },
                  {
                        "cert_id": "……",
                        "cert_data":
"MIICzDCCAnOgAwIBAg",
                        "chain_data": {
                              "ca_cert":
"MIIAHDFKBTkeKwIBAu",
                              "root_cert":
"MIIAAJFNCTuwUoPlat"
                        },
                        "serial_number":
"52341c3f9dcs2371"
                  }
            ]
      }
}
```

3. API ký tài liệu



a. Phương thức: POST

b. Đường dẫn: https://esign.neac.gov.vn/sign_v2/sign

c. Đặc tả:

- Tham số đầu vào:

TT	Tham số	Kiểu dữ liệu	Bắt buộc	Chú thích
1	sp_id	string	☑	Username do Cổng eSign cung cấp cho Cổng DVC
2	sp_password	string	☑	Password do Cổng eSign cung cấp cho Cổng DVC
3	user_id	string	☑	Số CCCD/CMND/Hộ chiếu/Mã số thuế/ của cá nhân/tổ chức muốn đăng nhập
4	data_to_be_signed	string	☑	Chuỗi băm của tài liệu được yêu cầu ký số.
5	doc_id	string	☑	Mã định danh tài liệu yêu cầu ký số do Cổng DVC sinh ra.

6	file_type	string	☐	Loại file: xml/json/word/pdf/excel/…
7	sign_type	string	☐	Loại ký số: hash
8	serial_number	string	☑	Số xê-ri của chứng thư số *(trong trường hợp một chủ thể có nhiều chứng thư số)*
9	time_stamp	string	☐	Thời gian người dùng gửi yêu cầu ký số. Định dạng: YYYYMMddHHmmSS
10	ca_name	string	☑	Tên của CA công cộng mà Cổng DVC muốn kết nối.(Tham chiếu tên tại url: https://neac.gov.vn/vi/ca-cong-cong/)

- Ví dụ tham số đầu vào:

```
{
    "sp_id": " ……..",
    "sp_password": "……",
    "user_id": "……..",
    "ca_name": "……..",
    "sign_files" : [
    {
        "data_to_be_signed" :
"MUswGAYJKoZDv1Wg1L9X8A/lQJOlk30=",
        "doc_id": "8347534jdsnfjsydf",
        "file_type": "pdf",
        "sign_type": "data"
    }
    ],
    "serial_number": "……."
}
```

- Tham số đầu ra:

TT	Tham số	Kiểu dữ liệu	Chú thích
1	status_code	int	Mã request thành công hoặc mã lỗi tương ứng. VD: 200, 401, 403, 500…
2	message	string	Thông điệp thành công hoặc thông điệp lỗi tương ứng với mã trạng thái ở status_code
3	transaction_id	string	Mã định danh giao dịch khởi tạo bởi Cổng eSign

- Ví dụ tham số đầu ra:

```
{
  "status_code": 200
  "message": "Yêu cầu ký số tài liệu tiếp nhận thành
công",
        "data":    {
              "transaction_id": "1234556789",
              "signed_files": null
              }
}
```

4. API kiểm tra trạng thái giao dịch

a. Phương thức: POST

b. Đường dẫn: https://esign.neac.gov.vn/sign_v2/get_status

c. Đặc tả

- Tham số đầu vào:

TT	Tham số	Kiểu dữ liệu	Bắt buộc	Chú thích
1	sp_id	string	☑	Username do Cổng eSign cung cấp cho Cổng DVC
2	sp_password	string	☑	Password do Cổng eSign cung cấp cho Cổng DVC
3	user_id	string	☑	Số CCCD/CMND/Hộ chiếu/Mã số thuế/ của cá

				nhân/tổ chức muốn đăng nhập
4	ca_name	string	☑	Tên của CA công cộng mà Cổng DVC muốn kết nối.(Tham chiếu tên tại url: https://neac.gov.vn/vi/ca-cong-cong/)
5	transaction_id	string	☑	Mã giao dịch được khởi tạo bởi Cổng eSign

- Ví dụ tham số đầu vào:

```
{
    "sp_id": " ……..",
    "sp_password": "……..",
    "user_id": "……..",
    "ca_name": "……",
    "transaction_id": "……."
}
```

- Tham số đầu ra:

TT	Tham số	Kiểu dữ liệu	Chú thích
1	status_code	int	Mã request thành công hoặc mã lỗi tương ứng. VD: 200, 401, 403, 500…
2	message	string	Thông điệp thành công hoặc thông điệp lỗi tương ứng với mã trạng thái ở status_code
3	transaction_id	string	Mã định danh giao dịch khởi tạo bởi Cổng eSign
4	signatures	string	Dữ liệu chữ ký

- Ví dụ tham số đầu ra:

```
{
    "status_code": " 200,
```

```
      "data": "{
          "transaction_id": "c7eabdae-740e-4845-9bcd-
dc495562d0bf",
          "signatures": null
      },
      "message": "PENDING",
}
```

```
{
      "status_code": " 200,
      "data": "{
          "transaction_id": "c7eabdae-740e-4845-9bcd-
dc495562d0bf",
          "signatures": [
          {
            "doc_id": "30c-7401-2562",
                  "signature_value":
"A7WttpP9/+8hUpZI/…",
                  "transaction_id": null
           }
          ]
      },
      "message": "SUCCESS",
}
```