BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 769 /QĐ-BTTTT

Hà Nội, ngày 27 tháng 4 năm 2022

QUYẾT ĐỊNH

Ban hành hướng dẫn kết nối ứng dụng sử dụng chữ ký số với tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng đối với hình thức ký số từ xa

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Nghị định số 130/2018/NĐ-CP ngày 27 tháng 9 năm 2018 của Chính phủ quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số;

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Thông tư số 16/2019/TT-BTTTT ngày 05 tháng 12 năm 2019 của Bộ trưởng Bộ Thông tin và Truyền thông quy định danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa;

Theo đề nghị của Giám đốc Trung tâm Chứng thực điện tử quốc gia.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Hướng dẫn kết nối ứng dụng sử dụng chữ ký số với tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng đối với hình thức ký số từ xa.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Chánh Văn phòng, Giám đốc Trung tâm Chứng thực điện tử quốc gia, Thủ trưởng các đơn vị thuộc Bộ, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ trưởng Nguyễn Mạnh Hùng;
- Các Thứ trưởng;
- Cổng thông tin điện tử của Bộ;
- Lưu: VT, NEAC.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

HƯỚNG DẪN KẾT NỐI ỨNG DỤNG SỬ DỤNG CHỮ KÝ SỐ VỚI TỔ CHỨC CUNG CẤP DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG ĐỐI VỚI HÌNH THỨC KÝ SỐ TỪ XA

(Ban hành kèm theo Quyết định số 769 /QĐ-BTTTT ngày 27 tháng 9 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. Giới thiệu

Hướng dẫn này là đặc tả các giao thức kết nối để chuyển yêu cầu ký số từ một dịch vụ/ứng dụng có kết nối mạng (SP) đến Tổ chức cung cấp dịch vụ chứng thực chữ ký số (CA) và nhận lại chứng thư số của người ký, kết quả ký số.

Hướng dẫn này không áp dụng đối với các dịch vụ/ứng dụng đã tích hợp chức năng ký số, các phần mềm ký số.

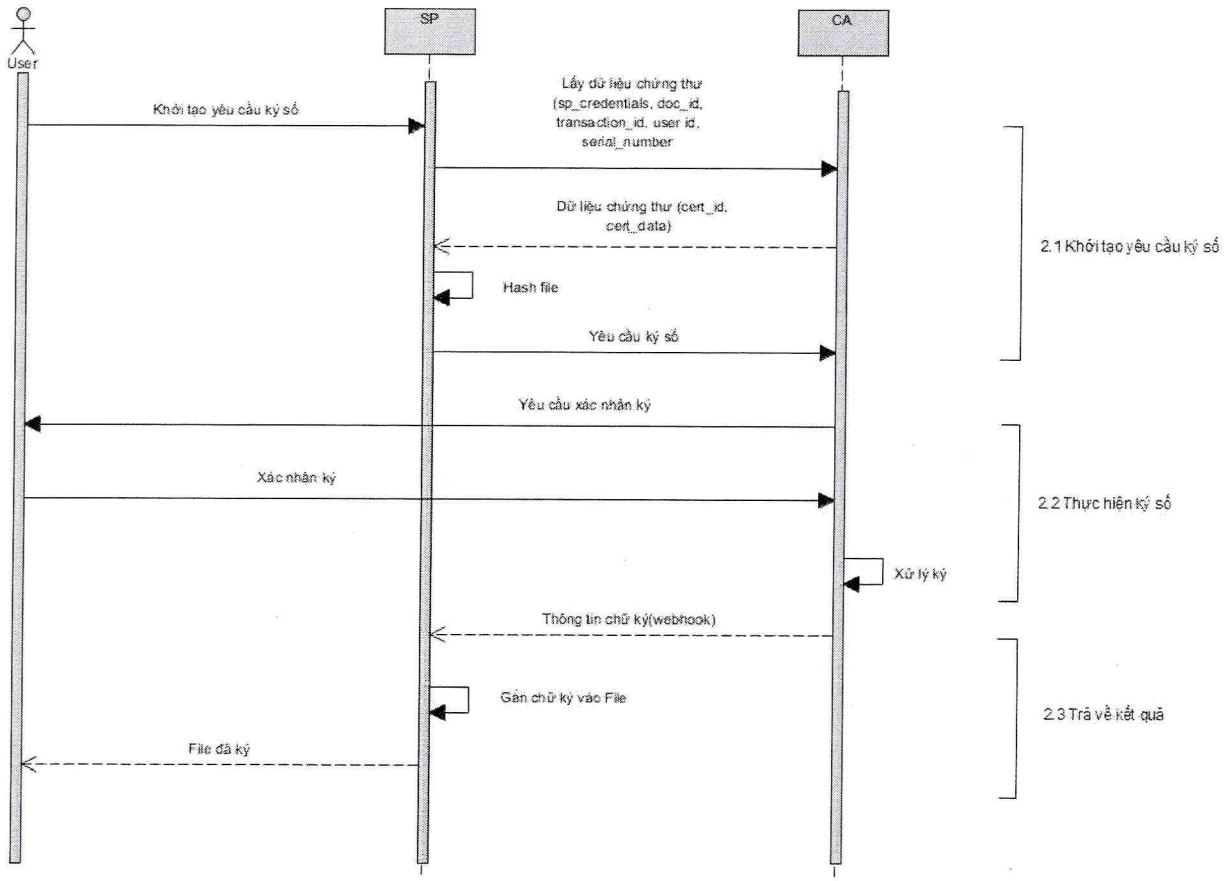
Trong trường hợp pháp luật chuyên ngành có quy định về định dạng của dữ liệu thì áp dụng trực tiếp quy định đó.

Giao thức này có thể được ứng dụng để thực hiện các hành động khác của người dùng (đăng ký, đăng nhập,...).

Do đặc thù của ký số từ xa cần phải có sự xác nhận của người sử dụng thông qua một phương tiện điện tử khác nên giao thức ký được miêu tả theo tài liệu là giao thức ký không đồng bộ. Tức là giữa SP và CA không duy trì kết nối trong quá trình CA xác thực với người dùng. Sau khi người dùng xác thực ký, kết quả ký số sẽ được CA trả về trên một kết nối khác tuân theo phương thức kết nối webhook như mô tả trong tài liệu này. Tuy nhiên, trong trường hợp khả thi, SP và CA được khuyến khích duy trì kết nối khoá phiên theo chuẩn TLS.

II. Đặc tả chi tiết

1. Sơ đồ



Hình 1. Sơ đồ luồng kết nối ký số tài liệu

2. Luồng xử lý yêu cầu ký số

2.1. Khởi tạo yêu cầu ký số

Người sử dụng thực hiện yêu cầu ký số.

SP đóng gói dưới dạng .xml (hoặc json) yêu cầu ký số bao gồm: thông tin xác thực tài khoản của SP (sp_credentials), mã tài liệu (doc_id), mã giao dịch (transaction_id), mã định danh người ký trong hệ thống SP (user_id), số xê-ri của chứng thư số (serial_number, trường hợp người dùng có nhiều hơn 01 chứng thư số), thời gian thực hiện yêu cầu.

SP gửi dữ liệu đã được đóng gói theo giao thức TLS cho CA.

SP gọi CA để lấy thông tin chứng thư.

SP tiến hành băm tài liệu cần được ký số và nén dữ liệu.

SP gửi mã băm (file_hash), thông tin xác thực tài khoản của SP (sp_credentials), mã giao dịch (transaction_id) cho CA.

2.2. Thực hiện ký số

CA bóc tách thông tin các thông tin trong dữ liệu .xml (hoặc json).

CA xác thực sp_credentials.

CA tìm thuê bao từ user_id, gửi lại chứng thư số cho SP.

CA gửi yêu cầu và nhận lại xác nhận ký đến người dùng (thông qua app của CA) để thực hiện quy trình ký số.

CA thực hiện cấp dấu thời gian cho giao dịch (nếu có).

2.3. Trả kết quả

CA đóng gói kết quả ký số dưới dạng .xml (hoặc json), gồm: chữ ký số theo từng mã tài liệu (doc_id), chứng thư số của người ký (user_cert), dấu thời gian (nếu có), thời gian thực hiện yêu cầu, mã giao dịch (transaction_id).

CA gửi dữ liệu đã được đóng gói theo giao thức TLS cho SP.

SP gắn chữ ký vào file và hoàn tất quy trình ký.

Hình thức trả:

Thông qua cơ chế webhook: Khi có kết quả ký tài liệu, CA sẽ gửi kết quả cho SP theo url webhook SP đăng ký trước với CA.

3. Định nghĩa giao thức

3.1. API lấy thông tin chứng thư

Mô tả:

- SP gọi CA.

- Khi người dùng tạo yêu cầu ký số, SP gọi CA để lấy dữ liệu chứng thư người dùng.

- CA sẽ kiểm tra và trả về danh sách chứng thư của người dùng.

- Khi có thông tin chứng thư, SP sử dụng dữ liệu này để tính toán hash file cần ký.

a. Đặc tả API

Phương thức: GET

Đường dẫn: https://x.x.x.x/get_certificate (x.x.x.x là URL API sẽ do mỗi CA tự quyết định)

Tham số đầu vào:

STT	Tham số	Kiểu dữ liệu	Bắt buộc	Chú thích
1	sp_id	String	✓	Tên tài khoản của SP do CA cung cấp
2	sp_password	String	✓	Mật khẩu do CA cung cấp cho SP
3	user_id	String	✓	Số CCCD/CMND/Hộ chiếu/Mã số thuế/ của cá nhân/tổ chức muốn đăng nhập
4	serial_number	String		Số xê-ri của chứng thư số
5	transaction_id	String	✓	Mã giao dịch khởi tạo bởi SP

Ví dụ tham số đầu vào:

```
{
    "sp_id": "DVCQG",
    "sp_password": "12345678",
    "user_id": "987654321",
    "transaction_id": "CA101003"
}
```

Tham số đầu ra:

STT	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	Raw data chứng thư (dạng base64)

5	chain_data	List<String>	List chứng thư, gồm 3 phần tử. Phần tử đầu tiên là chứng thư số người ký, thứ hai là chứng thư số của CA, cuối cùng là chứng thư số root do NEAC cấp.
6	serial_number	String	Số xê-ri của chứng thư số
7	transaction_id	String	Mã giao dịch khởi tạo bởi SP

Ví dụ tham số đầu ra:


```
{
   "status_code": 200,
   "message": "Lấy chứng thư thành công",
   "data":{
      "user_certificates": [
        {
            "cert_id": "123abc456",
            "cert_data": "MIIkiahfhare==",
            "chain_data": [
                "MIIakjfakurie2123=",
                "MIIakjfadauw73das=",
                "MII219nasu7as323n="
            ],
            "serial_number": "5Chsdfgh",
        },
        {
            "cert_id": "456cba123",
            "cert_data": "MII19ndja82b214b==",
            "chain_data": [
                "MIIakjfakurie2123=",
                "MIIakjfadauw73das=",
                "MII219nasu7as323n="
            ],
            "serial_number": "5Chsdfgh",
            "transaction_id": "CA101003"
        }
      ]
   }
}
```


3.2. API ký số tài liệu

a. <u>Mô tả</u>

- SP gọi CA, cung cấp mã giao dịch *(transaction_id)*
- SP dùng dữ liệu chứng thư người dùng để tính toán mã băm của tệp cần ký.
- SP gửi dữ liệu file_hash đến CA để thực hiện ký số tài liệu.
- SP sử dụng mã giao dịch để lấy thông tin chữ ký khi cần.
- Trong trường hợp đặc thù cần thiết, SP và CA có thể trao đổi thêm để trả về luôn kết quả ký tại request này (giữ và chờ request).

b. Đặc tả API

Phương thức: POST

Đường dẫn: https://x.x.x.x/sign (x.x.x.x là URL API sẽ do mỗi CA tự quyết định)

Tham số đầu vào:

STT	Tham số	Kiểu dữ liệu	Bắt buộc	Chú thích
1	sp_id	String	✓	Tên tài khoản của SP do CA cung cấp
2	sp_password	String	✓	Mật khẩu do CA cung cấp cho SP
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 biểu diễn của tài liệu được yêu cầu ký số (base64 string với file, hex với hash)
5	doc_id	String	✓	Mã tài liệu yêu cầu ký số (Mã này cần được hiển thị đồng thời tại giao diện của SP và tại giao diện tại ứng dụng của CA khi người dùng thực hiện xác thực yêu cầu ký số)
6	file_type	String	✓	Loại file: xml/json/word/pdf/excel/…
7	sign_type	String	✓	Loại ký số: hash/file
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	transaction_id	String	✓	Mã giao dịch khởi tạo bởi SP

Lưu ý: Truyền *data_to_be_signed* dạng base64 dung lượng tăng thêm 30%, khuyến nghị sử dụng mã băm (hash) trong việc chuyển yêu cầu ký.

Ví dụ tham số đầu vào:

```
{
    "sp_id": "DVCQG",
    "sp_password": "12345678",
    "user_id": "987654321",
    "transaction_id": "CA101003",
```

```
    "sign_files": [
        {
            "data_to_be_signed": "AyxHmaxJx=",
            "doc_id": "fc077be1-7e98-4055-89f1-056de9d923a6",
            "file_options": {
                "file_type": "xml",
                "sign_type": "hash"
            }
        },
        {
            "data_to_be_signed": "AyxHmaxJx=",
            "doc_id": "a2240e75-700e-4fa7-bac4-adc66358f26b",
            "file_options": {
                "file_type": "pdf",
                "sign_type": "hash"
            }
        },
    ],
    "serial_number": "5Chsdfgh",
    "time_stamp": "20211123070000Z"
}
```


Tham số đầu ra:

STT	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 giao dịch khởi tạo bởi SP
4	doc_id	String	Mã tài liệu yêu cầu ký số (Mã này cần được hiển thị đồng thời tại giao diện của SP và tại giao diện tại ứng dụng của CA khi người dùng thực hiện xác thực yêu cầu ký số)
5	signature_value	String	Dữ liệu chữ ký gắn với tài liệu (dạng base64)
6	timestamp_signature	String	Chữ ký của CA lên dấu thời gian của giao dịch ký số

Ví dụ tham số đầu ra:

a. Đối với trường hợp ký không đồng bộ:


```
{
   "status_code": 200
   "message": "Đã tiếp nhận tài liệu cần ký số",
   "data":{
      "transaction_id": "CA101003",
      "signed_files": null
   }
}
```

b. Đối với trường hợp ký đồng bộ: Khi theo cơ chế đồng bộ (giữ request ký và chờ xác nhận của người dùng) thì CA sẽ trả về kèm theo dữ liệu ký số file ở trường *signed_files*. Thời gian chờ xác nhận của người dùng phụ thuộc vào chính sách của từng CA. Sau khi hết thời gian chờ xác nhận, phiên giao dịch sẽ bị hủy bởi SP và yêu cầu ký số được xem là không thành công.

```
{
   "status_code": 200
   "message": "Ký số tài liệu thành công",
   "data":
{
      "transaction_id": "CA101003",
      "signed_files": [
         {
            "doc_id": "fc077be1-7e98-4055-89f1-056de9d923a6",
            "signature_value": "AyxHafsd323dssamaxJx=",
            "timestamp_signature": "20211123070000Z"
         },
         {
            "doc_id": "a2240e75-700e-4fa7-bac4-adc66358f26b",
            "signature_value": "Ayssgr43gsdgxHmaxJx=",
            "timestamp_signature": "20211123070000Z"
         }
      ]
   }
}
```

3.3. API webhook nhận thông tin ký tài liệu

a. <u>Mô tả</u>

- CA gọi SP theo url đăng ký trước.
- Sau khi CA có kết quả ký số tài liệu, CA sẽ gửi kết quả về cho SP.
- SP gắn chữ ký vào file, trả về cho người dùng, kết thúc luồng ký.

b. <u>Đặc tả API</u>

Phương thức: POST

Đường dẫn: https://x.x.x.x/recv_signature (x.x.x.x là URL API sẽ do mỗi CA tự quyết định)

Tham số đầu vào:

STT	Tham số	Kiểu dữ liệu	Bắt buộc	Chú thích
1	sp_id	String	✓	Tên tài khoản của SP do CA cung cấp (SP có thể dùng để phân biệt request của CA nào gửi về)
2	status_code	int	✓	Mã request thành công hoặc mã lỗi tương ứng. VD: 200, 401, 403, 500…
3	message	String	✓	Thông điệp thành công hoặc thông điệp lỗi tương ứng với mã trạng thái ở status_code

4	transaction_id	String	✓	Mã giao dịch khởi tạo bởi SP
5	doc_id	String		Mã tài liệu yêu cầu ký số
6	signature_value	String		Dữ liệu chữ ký gắn với tài liệu (dạng base64)
7	timestamp_signature	String		Chữ ký của CA lên dấu thời gian của giao dịch ký số

Ví dụ tham số đầu vào:

```
{
    "sp_id":"DVCQG",
    "status_code": 200
    "message": "Ký số thành công",
    "data": {
        "transaction_id":"CA101003",
        "signed_files": [
            {
                "doc_id":"fc077be1-7e98-4055-89f1-056de9d923a6",
                "signature_value":"AyxHafsd323dssamaxJx=",
                "timestamp_signature":"20211123070000Z"
            },
            {
                "doc_id":"a2240e75-700e-4fa7-bac4-adc66358f26b",
                "signature_value":"Ayssgr43gsdgxHmaxJx=",
                "timestamp_signature":"20211123070000Z"
            }
        ]
    }
}
```

Tham số đầu ra:

STT	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

Ví dụ tham số đầu ra:

```
{
    "status_code": 200
    "message": "Ký số thành công"
}
```

3.4. 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	403	Chứng thư bị thu hồi hoặc không rõ định dạng
5	500	Lỗi hệ thống
	…	Các lỗi khác (Nếu có)

- Bảng mã lỗi này tượng trưng cho các nhóm mã trạng thái cơ bản: thành công (mã 2xx, ví dụ 201,202…), không hợp lệ do phía người dùng (mã 4xx, ví dụ 401, 402…) và lỗi hệ thống (mã 5xx, ví dụ 500, 503…).

- Nếu CA có hệ thống mã trạng thái riêng thì có thể áp dụng hệ thống mã trạng thái đó, nhưng bắt buộc phải có đầy đủ 5 nhóm mã trạng thái cơ bản như trên và phải được công bố cho các bên muốn kết nối.

III. Chính sách

1. Trách nhiệm chung:

Trách nhiệm giữa tổ chức cung cấp dịch vụ (SP) và tổ chức cung cấp dịch vụ chứng thực ký số cộng cộng (CA) khi sử dụng giao thức quy định tại hướng dẫn này:

- SP và CA có trách nhiệm thỏa thuận SP_credentials với độ an toàn phù hợp với yêu cầu kỹ thuật được nêu chi tiết ở Phụ lục, quản lý và sử dụng an toàn, bí mật thông tin này.

- SP và CA có trách nhiệm thống nhất về các địa chỉ URL dành cho yêu cầu ký số, mã trạng thái và thông điệp trong trường hợp kết nối thành công cũng như lỗi.

- SP và CA có trách nhiệm thiết lập đường truyền TLS trong việc truyền, nhận dữ liệu, tránh trường hợp bị tấn công dẫn đến lộ, lọt dữ liệu.

2. Trách nhiệm của SP:

- Xác thực và chịu trách nhiệm về thông tin được truyền tải;

- Bảo mật thông tin của người dùng khi nhận được chứng thư số;

- Có phương án ngăn chặn việc lạm dụng giao thức này cho các mục đích khác, bảo vệ quyền lợi người dùng.

3. Trách nhiệm của CA:

- Đảm bảo tính sẵn sàng của dịch vụ ký số để phục vụ nhu cầu của SP.

- Đảm bảo hệ thống ký số đáp ứng các tiêu chuẩn.

YÊU CẦU KỸ THUẬT

STT	Nội dung	Yêu cầu kỹ thuật
1	sp_credentials	Chuẩn bị, thực thi và so sánh chuỗi username và password (theo RFC 8265)
2	Mã băm (hash)	Mã băm phải đạt được ít nhất độ an toàn theo chuẩn băm SHA (theo RFC 6234) hoặc cao hơn.
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	Kết nối đạt chuẩn an toàn tầng giao vận TLS 1.3(theo RFC 8446)
5	Hex	Chuẩn mã hóa base16, base32 và base64 (theo RFC 4648)
6	Chứng thư số của người dùng	Chứng thư số đạt chuẩn x509 (theo RFC 5280)