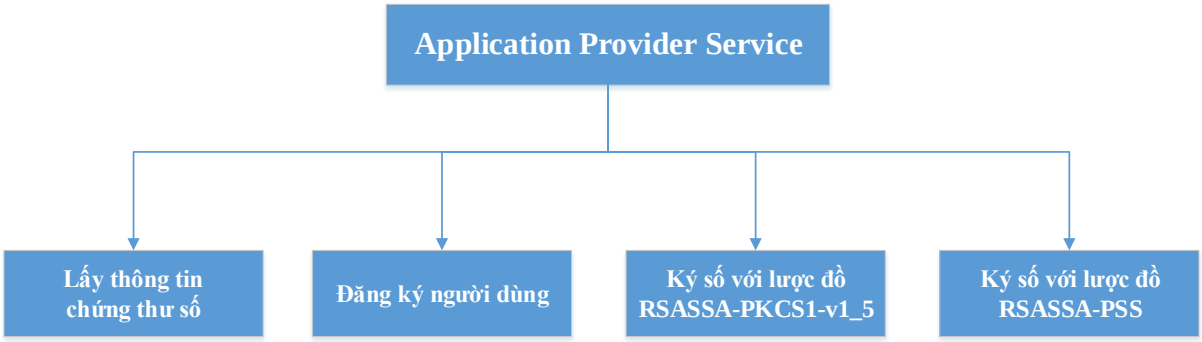
TÀI LIỆU HƯỚNG DẪN TÍCH HỢP
APPLICATION PROVIDER SERVICE

Contents

1. Mô hình chức năng của AP 2
2. Hàm lấy thông tin chứng thư số (GetCert) 2
3. Hàm ký số với lược đồ RSASSA-PKCS1-v1_5 (Sign) 3
4. Hàm ký số với lược đồ RSASSA-PSS (SignPSS) 4

1. Mô hình chức năng của AP



- AP service sử dụng giao thức SOAP, được thiết kế với bốn hàm chức năng chính đó là:

Chức năng	Thông tin	Ghi chú
Lấy thông tin chứng thư số (GetCert)	Hàm lấy thông tin chứng thư số tương ứng với số điện thoại của người dùng	Tham số đầu vào là số điện thoại của người dùng. Kết quả trả về nội dung chứng thư số dưới dạng BASE64
Đăng ký người dùng (Register)	Hàm đăng ký số điện thoại và chứng thư số của người dùng với hệ thống	Yêu cầu đăng ký cần phải được ký số bởi người quản trị
Ký số với lược đồ RSASSA-PKCS1-v1_5 (Sign)	Hàm ký số với lược đồ RSASSA-PKCS1-v1_5.	Tham số đầu vào là số điện thoại của người dùng và nội dung dữ liệu cần ký số
Ký số với lược đồ RSASSA-PSS (SignPSS)	Hàm ký số với lược đồ RSASSA-PSS	Tham số đầu vào là số điện thoại của người dùng và nội dung dữ liệu cần ký số

- AP service hỗ trợ giao thức bảo mật và xác thực kênh truyền SSL v3 và TLS v1.2

2. Hàm lấy thông tin chứng thư số (GetCert)

- Cấu trúc gói tin yêu cầu lấy chứng thư số lên AP service:

```
POST /APWS.asmx HTTP/1.1
Host: cms.ca.gov.vn
Content-Type: application/soap+xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
```

```
<soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
  <soap12:Body>
    <GetCert xmlns="http://ca.gov.vn/">
      <phone>string</phone>
    </GetCert>
  </soap12:Body>
</soap12:Envelope>
```

- Cấu trúc gói tin nhận kết quả trả về:

```
HTTP/1.1 200 OK
Content-Type: application/soap+xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
  <soap12:Body>
    <GetCertResponse xmlns="http://ca.gov.vn/">
      <GetCertResult>string</GetCertResult>
    </GetCertResponse>
  </soap12:Body>
</soap12:Envelope>
```

3. Hàm ký số với lược đồ RSASSA-PKCS1-v1_5 (Sign)

- Cấu trúc gói tin yêu cầu ký số:

```
POST /APWS.asmx HTTP/1.1
Host: cms.ca.gov.vn
Content-Type: application/soap+xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
  <soap12:Body>
    <Sign xmlns="http://ca.gov.vn/">
      <phone>string</phone>
      <messageToBeDisplayed>string</messageToBeDisplayed>
      <message>base64Binary</message>
```

```
    </Sign>
  </soap12:Body>
</soap12:Envelope>
```

Yêu cầu ký số có ba tham số đó là: phone là số điện thoại người ký, *messageToBeDisplayed* là thông điệp hiển thị trên điện thoại có SIM PKI thực hiện ký số, *message* là nội dung dữ liệu cần ký số dưới dạng BASE64.

- Cấu trúc gói tin kết quả trả về:

```
HTTP/1.1 200 OK
Content-Type: application/soap+xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
  <soap12:Body>
    <SignResponse xmlns="http://ca.gov.vn/">
      <SignResult>base64Binary</SignResult>
    </SignResponse>
  </soap12:Body>
</soap12:Envelope>
```

Kết quả trả về là định dạng Base64 của giá trị chữ ký số.

4. Hàm ký số với lược đồ RSASSA-PSS (SignPSS)

- Cấu trúc gói tin yêu cầu ký số:

```
POST /APWS.asmx HTTP/1.1
Host: cms.ca.gov.vn
Content-Type: application/soap+xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
  <soap12:Body>
    <SignPSS xmlns="http://ca.gov.vn/">
      <phone>string</phone>
      <messageToBeDisplayed>string</messageToBeDisplayed>
      <message>base64Binary</message>
    </SignPSS>
  </soap12:Body>
```

```
</soap12:Envelope>
```

Yêu cầu ký số có ba tham số đó là: phone là số điện thoại người ký, *messageToBeDisplayed* là thông điệp hiển thị trên điện thoại có SIM PKI thực hiện ký số, *message* là nội dung dữ liệu cần ký số dưới dạng BASE64.

- Cấu trúc gói tin kết quả trả về:

```
HTTP/1.1 200 OK
Content-Type: application/soap+xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
  <soap12:Body>
    <SignPSSResponse xmlns="http://ca.gov.vn/">
      <SignPSSResult>base64Binary</SignPSSResult>
    </SignPSSResponse>
  </soap12:Body>
</soap12:Envelope>
```

Kết quả trả về là định dạng Base64 của giá trị chữ ký số.