

TÀI LIỆU ĐẶC TẢ TÍCH HỢP VỚI HỆ THỐNG KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG

Mục lục

1. GIỚI THIỆU CHUNG.....	4
1.1. MỤC ĐÍCH TÀI LIỆU	4
1.2. ĐỐI TƯỢNG SỬ DỤNG.....	4
1.3. TỔNG QUAN TÀI LIỆU	4
1.4. THUẬT NGỮ	4
2. MÔ TẢ HỆ THỐNG DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG.....	5
2.1. SƠ ĐỒ KẾT NỐI HỆ THỐNG DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG	5
2.1.1. Sơ đồ kết nối	5
2.1.2. Mô tả các thành phần trong sơ đồ.....	6
2.2. MÔ TẢ CƠ CHẾ XÁC THỰC SSL 2 CHIỀU	6
3. MÔ TẢ GIAO TIẾP VỚI HỆ THỐNG DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG CLIENT WEB SERVICE	7
3.1. CẤU TRÚC MỘT YÊU CẦU (REQUEST) CLIENT GỬI LÊN SERVER.....	7
3.2. PHƯƠNG THỨC XỬ LÝ YÊU CẦU TỪ CLIENT	8
3.2.1. Phương thức processData	8
3.2.2. Nguyên mẫu của hàm	8
3.2.3. Tham số	8
a. Request	8
b. Response.....	8
3.2.4. Mô tả dữ liệu XML	9
a. AgreementHandler - Đăng ký hợp đồng sử dụng DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG	9
b. AgreementHandler - Thay đổi thông tin hợp đồng DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG.....	13
c. AgreementHandler - Thay đổi trạng thái hợp đồng DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG.....	16
d. AgreementHandler – Lấy thông tin hợp đồng.....	18

e.	AgreementHandler – Đổi mật khẩu SignServer	20
f.	AgreementHandler – Khôi phục mật khẩu SignServer	22
g.	AgreementHandler – Bật/Tắt chức năng ký SignServer	23
h.	AgreementHandler - Xác thực hợp đồng PKI	25
i.	OATHValidator - Xác thực mã OTP.....	Error! Bookmark not defined.
j.	OATHSync - Đồng bộ mã OTP	Error! Bookmark not defined.
k.	OATHRequest - Gửi yêu cầu lấy mã OTP (OATHRequest).....	Error! Bookmark not defined.
l.	OATHResponse - Xác thực mã OTP (OATHResponse) từ OATHRequest	Error! Bookmark not defined.
m.	MultiSigner - Ký văn bản (PDF, MS Office, OpenOffice, XML).....	26
n.	CMSSigner - Ký số chuẩn CAPICOM (CMS).....	30
o.	MultiValidator - Xác thực chữ ký trong văn bản (PDF, MS Office, OpenOffice, XML).....	32
p.	GeneralValidator – Xác thực chữ ký trong văn bản (PDF, MS Office, OpenOffice, XML) không quan tâm đến chứng thư số có trong hệ thống	34
q.	CapicomValidator - Xác thực chữ ký CAPICOM (CMS).....	36
r.	SignerAP - Ký file sử dụng SIM PKI - Mode bất đồng bộ	39
s.	SignatureValidator - Xác thực chữ ký sử dụng worker SignatureValidator.....	43
3.2.5.	<i>Danh sách các WorkerName được hỗ trợ trong hệ thống</i>	46
3.2.6.	<i>Thông tin CAGCredential</i>	47
3.2.7.	<i>Cách sử dụng các hàm trong lập trình.....</i>	48
4.	MÔ TẢ GIAO TIẾP VỚI HỆ THỐNG DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG ADMIN WEB SERVICE	51

1. GIỚI THIỆU CHUNG

1.1.MỤC ĐÍCH TÀI LIỆU

Tài liệu này được biên soạn nhằm mục đích đặc tả tích hợp với các hàm chức năng của hệ thống dịch vụ ký số trên thiết bị di động. Hệ thống này cung cấp các Web Method thực hiện những chức năng sau:

- Ký văn bản
- Xác thực (validate) chữ ký trên văn bản.
- Xác thực chữ ký PKI (Capicom signature).
- Các chức năng phục vụ cho phân quản trị và cấu hình.

1.2.ĐỐI TƯỢNG SỬ DỤNG

Tài liệu được cung cấp cho các đơn vị xây dựng hệ thống tích hợp vào hệ thống DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG để thực hiện ký, kiểm tra chữ ký trên văn bản.

1.3.TỔNG QUAN TÀI LIỆU

Tài liệu này bao gồm các thành phần sau:

- a. Giới thiệu về hệ thống DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG
- b. Sơ đồ kết nối hệ thống DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG
- c. Cơ chế xác thực SSL 2 chiều
- d. Mô tả giao tiếp với DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG Client Web Service dành cho phân hệ Font-End
- e. Mô tả giao tiếp với DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG Admin Web Service dành cho phân hệ Bac

1.4.THUẬT NGỮ

STT	Thuật ngữ	Diễn giải
1	CA	Certificate Authority
2	SSL	Secure Socket Layer
3	HTTPS	Hypertext Transfer Protocol Secure
4	JKS	Java KeyStore

STT	Thuật ngữ	Diễn giải
5	CSR	Certificate signing request
6	CRL	Certificate Revocation List

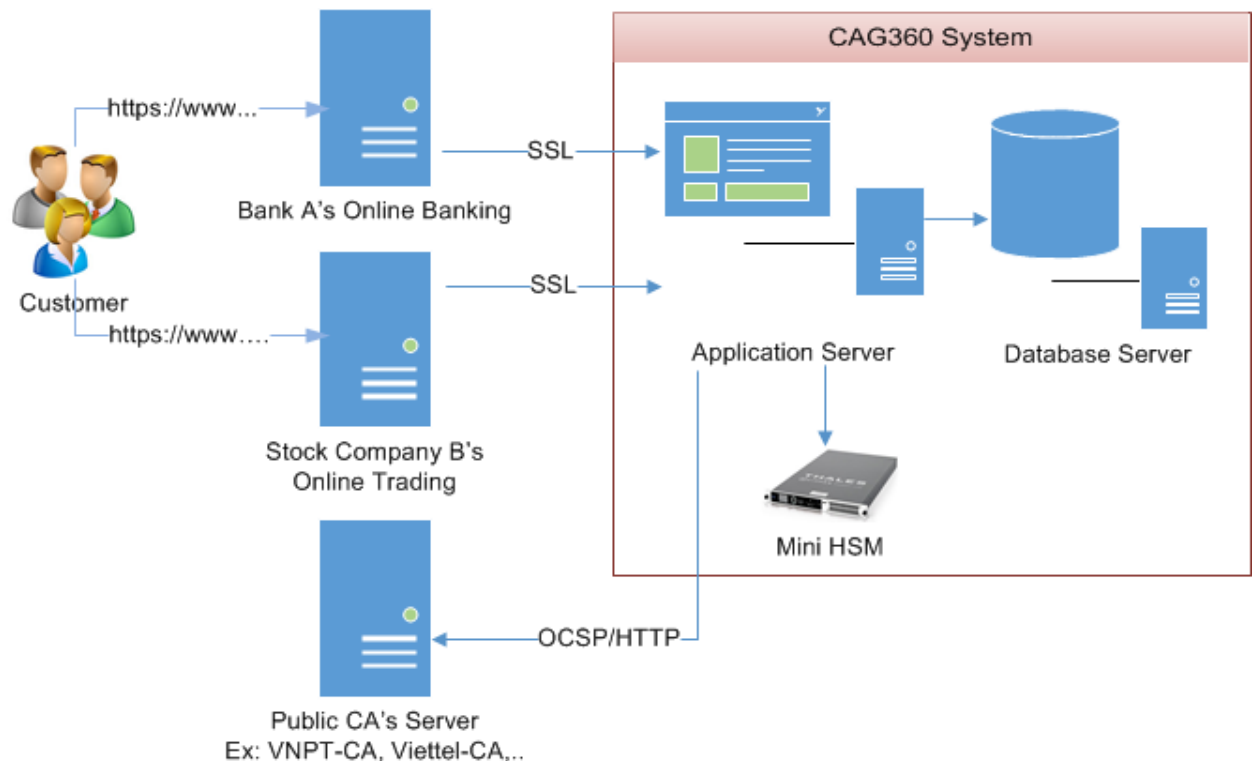
2. MÔ TẢ HỆ THỐNG DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG

DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG là một gateway đóng vai trò cung cấp các dịch vụ dành cho phân hệ Client và phân hệ Admin như sau:

- Phân hệ Client: thực hiện ký số và kiểm tra chữ ký số trên văn bản, xác thực chữ ký PKI.
- Phân hệ Admin: thực hiện cấu hình và cài đặt cho các hệ thống có sử dụng dịch vụ của DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG.

2.1. SƠ ĐỒ KẾT NỐI HỆ THỐNG DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG

2.1.1. Sơ đồ kết nối



Hình 1 - Sơ đồ kết nối hệ thống DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG

2.1.2. Mô tả các thành phần trong sơ đồ

Stt	Thành phần	Mô tả
1.	Hệ thống của khách hàng	Là hệ thống của các đơn vị sử dụng dịch vụ của hệ thống DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG, bao gồm hệ thống các Ngân hàng, Công ty chứng khoán,...
2.	CAs Server	Là hệ thống dịch vụ chứng thực chữ ký số chuyên dùng Chính phủ
3.	DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG Application Server	Là máy chủ ứng dụng của hệ thống DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG cung cấp các hàm Client Web Service và Admin Web Service. Các Service này hỗ trợ hình thức ký số bằng thiết bị HSM. Máy chủ này sẽ gọi đến các CAs Server để thực hiện kiểm tra trạng thái chứng thư số theo giao thức OCSP và download file CRL.
4.	DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG Database Server	Là máy chủ cơ sở dữ liệu hệ thống DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG dùng để lưu thông tin của hệ thống này.

2.2. MÔ TẢ CƠ CHẾ XÁC THỰC SSL 2 CHIỀU

Hệ thống DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG triển khai cơ chế xác thực SSL 2 chiều giữa Client và Server. Khi đó, dữ liệu trao đổi giữa Client và Server sẽ được mã hóa và bảo mật. Trong đó:

- Server: là JBoss Server, thực hiện quá trình xác thực Client. Nếu hợp lệ thì Server sẽ xử lý yêu cầu và trả kết quả về cho Client. Server được cấu hình giao thức HTTPS với

Keystore bao gồm file server.jks và truststore.jks. Ngoài ra, Server còn lưu chứng thư số của các nhà cung cấp chứng thư số cho Client.

- Client: là các hệ thống tích hợp với hệ thống DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG. Mỗi hệ thống tích hợp sẽ được cấp file JKS riêng. Mỗi Client được cấp một cặp khóa dạng tập tin mềm PKCS#12 (client.p12) để thực hiện quá trình bắt tay với Sever và ký thông tin yêu cầu xác thực (Phần II.2.1) gửi lên Server.

```
<Connector protocol="HTTP/1.1" SSLEnabled="true"
port="443" address="{jboss.bind.address}"
scheme="https" secure="true" clientAuth="true"
keystoreFile="{jboss.server.home.dir}/conf/serverkeystore.jks"
```

3. MÔ TẢ GIAO TIẾP VỚI HỆ THỐNG DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG CLIENT WEB SERVICE

DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG Client Web Service là một Web Service. Vì vậy, các Client giao tiếp với hệ thống DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG thông qua giao thức SOAP/HTTPS.

Địa chỉ kết nối Client Webservice thông thường sẽ là:

http://<YourIPServer>/Signing_Service/ClientWSService/ClientWS?wsdl

3.1.CÁU TRÚC MỘT YÊU CẦU (REQUEST) CLIENT GỬI LÊN SERVER

Client Web Service (ClientWS) cung cấp các Web Method thực hiện các tác vụ ký và xác thực văn bản. Một yêu cầu do Client gửi Server phải bao gồm các thành phần sau:

- Thông tin định danh Client (Credential): Thông tin này sẽ được đối tượng hóa thành đối tượng CAGCredential, chứa thông tin định danh cũng như xác thực Client.
- Thông tin phục vụ cho việc xử lý yêu cầu trên Server: Thông tin này dạng chuỗi XML, có các tag dữ liệu tương ứng phục vụ cho việc xử lý trên Server.

Sau đây là mô tả chi tiết từng thành phần.

3.2. PHƯƠNG THỨC XỬ LÝ YÊU CẦU TỪ CLIENT

3.2.1. Phương thức *processData*

Phương thức *processData* thực hiện các tác vụ ký và xác thực văn bản, xác thực chữ ký số PKI.

3.2.2. Nguyên mẫu của hàm

```
TransactionInfo processData(TransactionInfo transInfo);
```

3.2.3. Tham số

a. Request

TransactionInfo			
Kiểu dữ liệu	Tên tham số	Đặc tính	Mô tả
CAGCredential	cagCredential	Bắt buộc	Chứa thông tin định danh và xác thực Client. Cấu trúc đối tượng CAGCredential sẽ được trình bày ở mục 3.2.6
String	xmlData	Bắt buộc	Chuỗi XML chứa thông tin cần cho Server xử lý. Chi tiết sẽ được trình bày ở mục 3.2.4
byte[]	fileData	Tùy chọn	Tập tin cần cho Server ký hoặc xác thực. Chỉ cần thiết đối với tác vụ liên quan đến văn bản cần xử lý

b. Response

TransactionInfo			
Kiểu dữ liệu	Tên tham số	Đặc tính	Mô tả
String	xmlData		Chuỗi XML chứa thông tin cần cho Server xử lý. Chi tiết sẽ được trình bày ở mục 3.2.4
byte[]	fileData		Tập tin đã được ký

3.2.4. Mô tả dữ liệu XML

a. *AgreementHandler* - Đăng ký hợp đồng sử dụng DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG

Request

<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ID>01009090</ID>

<WorkerName>AgreementHandler</WorkerName>

<Action>REGISTRATION</Action>

<Expiration>720</Expiration>

<IsPKI>True</IsPKI>

<Certificate>MIIFQDCCBCig...rYw==</Certificate>

<IsLCDPKI>True</IsLCDPKI>

<LCDPKICertificate>MIH...wrYw==</LCDPKICertificate>

<IsPKISim>True</IsPKISim>

<PKISim>84940000001</PKISim>

<PKISimVendor>VIETTEL</PKISimVendor>

<DisplayMessage>Xac nhan ky tai lieu</DisplayMessage>

<IsPKISigning>True</IsPKISigning>

<WorkerNameSigning></WorkerNameSigning>

<SPKIEmail>emailpki@gmail.com</SPKIEmail>

<SKeyName>TRUSTEDHUB-105442939-20170926</SKeyName>

<SKeyType>0</SKeyType>

Response

<Channel> TRUSTEDHUB </Channel>

<User>111488361</User>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS </ResponseMessage>

<BillCode>20141020165230736540</BillCode>

<AgreementStatus>ACTIVE</AgreementStatus>

Mô tả

Thuộc tính	Đặc tính	Diễn giải
------------	----------	-----------

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request
	Action	Bắt buộc	Hành động sẽ xử lý đối với hợp đồng: <ul style="list-style-type: none"> REGISTRATION UNREGISTRATION CHANGEINFO VALIDATION
	Expiration	Bắt buộc	Thời hạn hợp đồng (ngày). Khuyến khích để 36500 (100 năm)
	IsPKI	Tùy chọn	True: Sử dụng dịch vụ xác thực PKI False: Không sử dụng dịch vụ xác thực PKI
	Certificate	Tùy chọn	Chứng thư số đăng ký sử dụng dịch vụ xác thực PKI
	IsLCDPKI	Tùy chọn	True: Sử dụng dịch vụ xác thực LCD PKI Token False: Không sử dụng dịch vụ xác thực LCD PKI Token
	LCDPKICertificate	Tùy chọn	Chứng thư số đăng ký sử dụng dịch vụ xác thực LCD PKI Token
	IsPKISim	Tùy chọn	True: Sử dụng dịch vụ ký số PKI SIM

Thuộc tính		Đặc tính	Diễn giải
			False: Không sử dụng dịch vụ ký số PKI SIM
	DisplayMessage	Tùy chọn	Thông tin sẽ hiển thị ở điện thoại khách hàng
	PKISim	Tùy chọn	Số điện thoại sử dụng dịch vụ ký số PKI SIM
	PKISimVendor	Bắt buộc	Nhà mạng cung cấp SIM: <ul style="list-style-type: none"> • VIETTEL • VINAPHONE • MOBIFONE
	IsPKISigning	Tùy chọn	True: Sử dụng dịch ký số tập trung SignServer False: Không sử dụng dịch ký số tập trung SignServer
	WorkerNameSigning	Bắt buộc	Tên Worker thực hiện ký số tập trung
	SPKIEmail	Bắt buộc	Địa chỉ email để khôi phục mật khẩu cho việc ký tập trung
	SKeyName	Bắt buộc	Tên khóa thực hiện ký số tập trung
	SKeyType	Bắt buộc	Loại khóa thực hiện ký số tập trung <ul style="list-style-type: none"> • 1: Khóa riêng (Định dạng: CHANNEL-USER-NGAYTAO) • 2: Khóa chia sẻ dùng trong Channel (Định dạng CHANNEL-NGAYTAO) 3: Khóa chia sẻ dùng giữa các Channel (Định dạng NGAYTAO)

Thuộc tính		Đặc tính	Diễn giải
	ResponseCode		Mã trạng thái trả về
	ResponseMessage		<ul style="list-style-type: none"> Diễn giải mã trạng thái trả về
	BillCode		BillCode của giao dịch
	AgreementStatus		Trạng thái hợp đồng sau khi được tạo thành công
			<ul style="list-style-type: none">
RESPONSE			

Lưu ý: Việc đăng ký hợp đồng có phương thức SignServer chỉ được thực hiện trên BackOffice.

b. AgreementHandler - Thay đổi thông tin hợp đồng DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG

Request

<Channel> TRUSTEDHUB </Channel>

<User>100310181</User>

<ID>01009090</ID>

<WorkerName>AgreementHandler</WorkerName>

<Action> CHANGEINFO </Action>

<IsExtend>True</IsExtend>

<Expiration>3</Expiration>

<IsPKI>True</IsPKI>

<Certificate>MIIDuTCCAqGgAwIBAgIQVAQ...</Certificate>

<IsLCDPKI>True</IsLCDPKI>

<LCDPKICertificate>MIIFQDCCBCigA...</LCDPKICertificate>

<IsPKISim>True</IsPKISim>

<PKISim>8494000001</PKISim>

<DisplayMessage>Đang ký hợp đồng sim pki</DisplayMessage>

Response

<Channel> TRUSTEDHUB </Channel>

<User>111488361</User>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS </ResponseMessage>

<BillCode>20141020165230736540</BillCode>

Mô tả

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thốngClient
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request

Thuộc tính		Đặc tính	Diễn giải
	Action	Bắt buộc	Hành động sẽ xử lý đối với hợp đồng: <ul style="list-style-type: none"> • REGISTRATION • UNREGISTRATION • CHANGEINFO • VALIDATION
	Expiration	Tùy chọn	Thời hạn hợp đồng (ngày)
	IsPKI	Tùy chọn	True: Sử dụng dịch vụ xác thực PKI False: Không sử dụng dịch vụ xác thực PKI
	Certificate	Tùy chọn	Chứng thư số đăng ký sử dụng dịch vụ xác thực PKI
	IsLCDPKI	Tùy chọn	True: Sử dụng dịch vụ xác thực LCD PKI Token False: Không sử dụng dịch vụ xác thực LCD PKI Token
	LCDPKICertificate	Tùy chọn	Chứng thư số đăng ký sử dụng dịch vụ xác thực LCD PKI Token
	IsPKISim	Tùy chọn	True: Sử dụng dịch vụ ký số PKI SIM False: Không sử dụng dịch vụ ký số PKI SIM
	DisplayMessage	Tùy chọn	Thông tin sẽ hiển thị ở điện thoại khách hàng
	PKISim	Tùy chọn	Số điện thoại sử dụng dịch vụ ký số PKI SIM
	ResponseCode		Mã trạng thái trả về
	ResponseMessage		Diễn giải mã trạng thái trả về

Thuộc tính		Đặc tính	Diễn giải
	BillCode		BillCode của giao dịch
RESPONSE			

c. AgreementHandler - Thay đổi trạng thái hợp đồng DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG

Request

<Channel> TRUSTEDHUB </Channel>

<User>111488361</User>

<ID>01009090</ID>

<WorkerName>AgreementHandler</WorkerName>

<Action>UNREGISTRATION</Action>

<AgreementStatus>CANC</AgreementStatus>

Response

<Channel> TRUSTEDHUB </Channel>

<User>111488361</User>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS </ResponseMessage>

<BillCode>20141020165230736540</BillCode>

Mô tả

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request
	Action	Bắt buộc	Hành động sẽ xử lý đối với hợp đồng: <ul style="list-style-type: none"> REGISTRATION UNREGISTRATION CHANGEINFO VALIDATION
	AgreementStatus	Bắt buộc	Trạng thái hợp đồng cần thay đổi: <ul style="list-style-type: none"> CANC: Hủy hợp đồng ACTIVATED: Kích hoạt hợp đồng BLOC: Khóa hợp đồng EXTE: Gia hạn hợp đồng EXPR: Hợp đồng hết hạn
RESPONSE	ResponseCode		Mã trạng thái trả về
	ResponseMessage		Diễn giải mã trạng thái trả về

Thuộc tính		Đặc tính	Diễn giải
	BillCode		BillCode của giao dịch

d. AgreementHandler – Lấy thông tin hợp đồng

Request

```
<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ID>01009090</ID>

<WorkerName>AgreementHandler</WorkerName>

<Action>GETAGREEMENT</Action>

<AgreementStatus>ACTIVATED</AgreementStatus>
```

Response

```
<Channel>TRUSTEDHUB</Channel>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS</ResponseMessage>

<BillCode>TRUSTEDHUB-105442939-20170926101318-13526</BillCode>

<NumOfAgreementFound>1</NumOfAgreementFound>

<Agreements>

  <Agreement>

    <User>105442939</User>

    <ID>01009090</ID>

    <Channel>TRUSTEDHUB</Channel>

    <AgreementStatus>ACTIVATED</AgreementStatus>

    <IsPKI>True</IsPKI>
```

```
<Certificate>MIIFSjCCAzKgAw...xAk=</Certificate>

<TPKITHumbPrint>E33E7180D0B22CA725F4C88AB5</TPKITHumbPrint>

<IsLCDPKI>True</IsLCDPKI>

<LCDPKICertificate>MIIE0TCCArmG...3+S6g==</LCDPKICertificate>

<LPKITHumbPrint> E33E7180D0B22CA725F4C88AB5</LPKITHumbPrint>

<IsPKISim>True</IsPKISim>

<PKISim>84940000002</PKISim>

<WPKICertificate>MIIEoDCCA4igAVAREW...jgpbv9</WPKICertificate>

<WPKITHumbPrint> E33E7180D0B22C5F4C88AB5</WPKITHumbPrint>

<IsSignServer>True</IsSignServer>

<IsRegistered>False</IsRegistered>

<SCertificate>MIIGwDCC...Yw==</SCertificate>

<CreateDate>05/07/2017</CreateDate>

<EffectiveDate>05/07/2017</EffectiveDate>

<ExpiredDate>25/06/2019</ExpiredDate>

</Agreement>

</Agreements>
```

Mô tả

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan

Thuộc tính		Đặc tính	Diễn giải
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request
	Action	Bắt buộc	Hành động sẽ xử lý đối với hợp đồng: <ul style="list-style-type: none"> GETAGREEMENT
	AgreementStatus	Bắt buộc	Trạng thái hợp đồng cần thay đổi: <ul style="list-style-type: none"> CANC: Hủy hợp đồng ACTIVATED: Kích hoạt hợp đồng BLOC: Khóa hợp đồng EXTE: Gia hạn hợp đồng EXPR: Hợp đồng hết hạn
RESPONSE	ResponseCode		Mã trạng thái trả về
	ResponseMessage		Diễn giải mã trạng thái trả về
	BillCode		BillCode của giao dịch
Thông tin của hợp đồng tương ứng.			

e. AgreementHandler – Đổi mật khẩu SignServer

Request

<Channel>TRUSTEDHUB</Channel>

<User>thanhtest74</User>

<ID>01009090</ID>

<WorkerName>AgreementHandler</WorkerName>

<Action>CHANGEINFO</Action>

<IsPKISigning>True</IsPKISigning>

<CurrentPassword>12345678</CurrentPassword>

<NewPassword>87654321</NewPassword>

Response

<Channel>TRUSTEDHUB</Channel>

<User>thanhtest74</User>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS</ResponseMessage>

<BillCode>TRUSTEDHUB-thanhtest74-20170926103336-13529</BillCode>

Mô tả

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request
	Action	Bắt buộc	Hành động sẽ xử lý đối với hợp đồng: <ul style="list-style-type: none"> CHANGEINFO
	IsPKISigning	Bắt buộc	Set lên True để xử lý hợp đồng SignServer
	CurrentPassword	Bắt buộc	Mật khẩu hiện tại
	NewPassword	Bắt buộc	Mật khẩu mới
ESP	ResponseCode		Mã trạng thái trả về

Thuộc tính		Đặc tính	Diễn giải
	ResponseMessage		Diễn giải mã trạng thái trả về
	BillCode		BillCode của giao dịch

f. AgreementHandler – Khởi phục mật khẩu SignServer

Request

<Channel>TRUSTEDHUB</Channel>
 <User>105442939</User>
 <ID>01009090</ID>
 <WorkerName>AgreementHandler</WorkerName>
 <Action>CHANGEINFO</Action>
 <IsPKISigning>True</IsPKISigning>
 <SetRecovery>True</SetRecovery>

Response

<Channel>TRUSTEDHUB</Channel>
 <User>105442939</User>
 <ResponseCode>0</ResponseCode>
 <ResponseMessage>SUCCESS</ResponseMessage>
 <BillCode>TRUSTEDHUB-thanhthtest74-20170926103336-13529</BillCode>

Mô tả

Thuộc tính		Đặc tính	Diễn giải
EQ	Channel	Bắt buộc	Mã hệ thống Client

Thuộc tính		Đặc tính	Diễn giải
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request
	Action	Bắt buộc	Hành động sẽ xử lý đối với hợp đồng: <ul style="list-style-type: none"> CHANGEINFO
	IsPKISigning	Bắt buộc	Set lên True để xử lý hợp đồng SignServer
	SetRecovery	Bắt buộc	True để thực hiện khôi phục mật khẩu. Mật khẩu mới sẽ được gửi vào email lúc đăng ký hợp đồng SignServer
RESPONSE	ResponseCode		Mã trạng thái trả về
	ResponseMessage		Diễn giải mã trạng thái trả về
	BillCode		BillCode của giao dịch

g. AgreementHandler – Bật/Tắt chức năng ký SignServer

Request

<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ID>01009090</ID>

<WorkerName>AgreementHandler</WorkerName>

<Action>CHANGEINFO</Action>

<IsPKISigning>True</IsPKISigning>

<IsRegistered>True</IsRegistered>

Response

<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS</ResponseMessage>

<BillCode>TRUSTEDHUB-thanhstest74-20170926103336-13529</BillCode>

Mô tả

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request
	Action	Bắt buộc	Hành động sẽ xử lý đối với hợp đồng: <ul style="list-style-type: none"> CHANGEINFO
	IsPKISigning	Bắt buộc	Set lên True để xử lý hợp đồng SignServer
	IsRegistered	Bắt buộc	True thực hiện bật tính năng ký số tập trung False thực hiện vô hiệu tính năng ký số tập trung
RESPONSE	ResponseCode		Mã trạng thái trả về
	ResponseMessage		Diễn giải mã trạng thái trả về
	BillCode		BillCode của giao dịch

h. AgreementHandler - Xác thực hợp đồng PKI

Request

<Channel>Dịch vụ ký số trên thiết bị di động</Channel>

<ID>01009090</ID>

<WorkerName>AgreementHandler</WorkerName>

<Action>VALIDATION</Action>

<Certificate>MIIDuTCCAqGgAwIBAgIQ...</Certificate>

Response

<Channel>Dịch vụ ký số trên thiết bị di động</Channel>

<User>111488361</User>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS </ResponseMessage>

<BillCode>20141020165230736540</BillCode>

Mô tả

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request
	Action	Bắt buộc	Hành động sẽ xử lý đối với hợp đồng: <ul style="list-style-type: none"> REGISTRATION UNREGISTRATION

Thuộc tính		Đặc tính	Diễn giải
			<ul style="list-style-type: none"> CHANGEINFO VALIDATION
	Certificate	Bắt buộc	Chứng thư số cần xác thực hợp đồng PKI
ESPONSE	ResponseCode		Mã trạng thái trả về
	ResponseMessage		Diễn giải mã trạng thái trả về
	BillCode		BillCode của giao dịch

i. MultiSigner - Ký văn bản (PDF, MS Office, OpenOffice, XML)

Request

<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ID>01009090</ID>

<FileType>pdf</FileType>

<MetaData>

<Method>SynchronousSign</Method>

<Password>12345678</Password>

<ExternalStorage>P2P</ExternalStorage>

<PageNo>1</PageNo>

<Coordinate>50,500,550,680</Coordinate>

<SignReason>Ký lần 2, sếp cho ý kiến</SignReason>

<VisibleSignature>True</VisibleSignature>

<SignerInfoPrefix>Sign by </SignerInfoPrefix>

<DateTimePrefix>Sign on </DateTimePrefix>

<SignReasonPrefix>Sign for </SignReasonPrefix>

<VisualStatus>True</VisualStatus>

<SignatureImage>iVBORw0KGgoAAA...gg==</SignatureImage>

<ImageAndText>True</ImageAndText>

</MetaData>

<WorkerName>MultiSigner</WorkerName>

Response

<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS</ResponseMessage>

<BillCode>TRUSTEDHUB-105442939-20170712145655-48</BillCode>

<FileType>pdf</FileType>

<SigningCertificate>MIIEKXWA++A2bGvuAXt5kg==</SigningCertificate>

Mô tả

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)

Thuộc tính		Đặc tính	Diễn giải
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	FileType	Bắt buộc	Kiểu file cần xử lý
	Method	Bắt buộc	Phương thức thực hiện ký số
	Password	Tùy chọn	Mật khẩu xác thực người dùng ký số tập trung. Nếu không truyền sẽ lấy mật khẩu mặc định của hệ thống.
	ExternalStorage	Tùy chọn	Tùy chọn nơi lấy File cần ký + P2P: File lưu trữ lại local + FILENET: File lưu trữ trên FileNet server
	PageNo	Tùy chọn	Trang cần đặt chữ ký
	Coordinate	Tùy chọn	Tọa độ chữ ký
	SignReason	Tùy chọn	Nội dung (lý do) ký
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request

Thuộc tính		Đặc tính	Diễn giải
	VisibleSignature	Tùy chọn	+ True: Hiển thị chữ ký trên file PDF + False: Chữ ký ẩn trên file PDF
	SignerInfoPrefix	Tùy chọn	Prefix trước thông tin của Signer. Ví dụ: signed by Công ty ABC
	DateTimePrefix	Tùy chọn	Prefix trước thông tin thời gian ký. Ví dụ: signed on 20-10-2018
	SignReasonPrefix	Tùy chọn	Prefix trước thông tin lý do ký. Ví dụ: nội dung ký phê duyệt TD
	ShowSignerInfoOnly	Tùy chọn	Chỉ hiển thị thông tin chủ thể ký (True/False)
	ShowDateTimeOnly	Tùy chọn	Chỉ hiển thị thông tin ngày ký (True/False)
	VisualStatus	Tùy chọn	Hiển thị Icon (validation symbol) xác thực
	SignatureImage	Tùy chọn	Base64 hình ảnh dùng trong chữ ký

Thuộc tính		Đặc tính	Diễn giải
	ImageAndText	Tùy chọn	+ True: Hiển thị hình ảnh (background) và chữ (signer info) + False: Chỉ hiển thị hình ảnh (background)
RESPONSE	ResponseCode		Mã trạng thái trả về
	ResponseMessage		Diễn giải mã trạng thái trả về
	BillCode		BillCode của giao dịch
	SigningCertificate		Chứng thư số dùng để ký file

j. CMSSigner - Ký số chuẩn CAPICOM (CMS)

Request

<Channel>Dịch vụ ký số trên thiết bị di động</Channel>

<User>111488361</User>

<ID>01009090</ID>

<FileType>txt</FileType>

<WorkerName>CMSSigner</WorkerName>

<DataToSign>data to sign</DataToSign>

Response

<Channel>Dịch vụ ký số trên thiết bị di động</Channel>

<User>111488361</User>

<ID>01009090</ID>

<ResponseCode>0</ResponseCode>

<ResponseMessage>OK</ResponseMessage>

<BillCode>20141020163542368605</BillCode>

<FileType>txt</FileType>

<SigningCertificate>MIIFoDCCA4igA...</SigningCertificate>

Mô tả

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	FileType	Bắt buộc	Kiểu file cần xử lý
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request
	DataToSign	Bắt buộc	Dữ liệu cần ký
RESPONSE	ResponseCode		Mã trạng thái trả về
	ResponseMessage		Diễn giải mã trạng thái trả về

Thuộc tính		Đặc tính	Diễn giải
			về
	BillCode		BillCode của giao dịch
	SigningCertificate		Chứng thư số dùng để ký dữ liệu

k. MultiValidator - Xác thực chữ ký trong văn bản (PDF, MS Office, OpenOffice, XML)

Request

```
<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ID>01009090</ID>

<MetaData>

<ExternalStorage>P2P</ExternalStorage>

<SignatureMethod>TPKI</SignatureMethod>

</MetaData>

<WorkerName>MultiValidator</WorkerName>
```

Response

```
<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS</ResponseMessage>

<BillCode>TRUSTEDHUB-105442939-20170704165508-51909</BillCode>

<SignerInfo>
```


<SerialNumber>54045346E3DD0D28B73BB03637ABDC4A</SerialNumber>

<SubjectName>Nguyễn Văn A</SubjectName>

<IssuerName>FPT-CA</IssuerName>

<DateValid>20/11/2012</DateValid>

<DateExpired>20/11/2013</DateExpired>

<SigningTime>20/12/2012 15:20:44</SigningTime>

</SignerInfo>

Mô tả

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	SignatureMethod	Bắt buộc	Phương thức xác thực chữ ký
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request
RESPONSE	ResponseCode		Mã trạng thái trả về
	ResponseMessage		Diễn giải mã trạng thái trả về
	BillCode		BillCode của giao dịch

Thuộc tính		Đặc tính	Diễn giải
	SignerInfo		Thông tin chữ ký trong văn bản
	SerialNumber		Định danh chứng thư số
	SubjectName		Tên chứng thư số
	IssuerName		Đơn vị cấp chứng thư số
	DateValid		Ngày có hiệu lực chứng thư số
	DateExpired		Ngày hết hạn chứng thư số

l. GeneralValidator – Xác thực chữ ký trong văn bản (PDF, MS Office, OpenOffice, XML) không quan tâm đến chứng thư số có trong hệ thống

Request

<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ID>01009090</ID>

<MetaData>

<ExternalStorage>P2P </ExternalStorage>

</MetaData>

<WorkerName>GeneralValidator</WorkerName>

Response

```
<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS</ResponseMessage>

<BillCode>TRUSTEDHUB-105442939-20170704165508-51909</BillCode>

<SignerInfo>

<SerialNumber>54045346E3DD0D28B73BB03637ABDC4A</SerialNumber>

  <SubjectName>Nguyễn Văn A</SubjectName>

  <IssuerName>VGCA</IssuerName>

  <DateValid>20/11/2012</DateValid>

  <DateExpired>20/11/2013</DateExpired>

  <SigningTime>20/12/2012 15:20:44</SigningTime>

</SignerInfo>
```

Mô tả

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	ExternalStorage	Bắt buộc	Tùy chọn nơi lấy File cần ký

Thuộc tính		Đặc tính	Diễn giải
			+ P2P: File lưu trữ lại local + FILENET: File lưu trữ trên FileNet server
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request
RESPONSE	ResponseCode		Mã trạng thái trả về
	ResponseMessage		Diễn giải mã trạng thái trả về
	BillCode		BillCode của giao dịch
	SignerInfo		Thông tin chữ ký trong văn bản
	SerialNumber		Định danh chứng thư số
	SubjectName		Tên chứng thư số
	IssuerName		Đơn vị cấp chứng thư số
	DateValid		Ngày có hiệu lực chứng thư số
	DateExpired		Ngày hết hạn chứng thư số

m. CapicomValidator - Xác thực chữ ký CAPICOM (CMS)

Request

```
<Channel> TRUSTEDHUB </Channel>

<User>106555642</User>

<ID>01009090</ID>

<WorkerName>CapicomValidator</WorkerName>

<MetaData>

  <SignedData>data</SignedData>

</MetaData>

<CapicomSignature>MIAGCSqGSIb3DQEHAqCAMIA...</CapicomSignature>
```

Response

```
<Channel> TRUSTEDHUB </Channel>

<User>106555642</User>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS</ResponseMessage>

<BillCode>20141020163903840317</BillCode>

<SignerInfo>

  <SerialNumber>5401cf4d80feedd9bc844</SerialNumber>

  <SubjectName>0100231226</SubjectName>

  <IssuerName>VNPT Certification Authority</IssuerName>

  <DateValid>07/07/2014</DateValid>

  <DateExpired>05/10/2014</DateExpired>

</SignerInfo>
```

Mô tả

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	SerialNumber	Tùy chọn	SerialNumber của CTS dùng để ký văn bản. Nếu giá trị này là null, hệ thống sẽ lấy SerialNumber của CTS lúc đăng ký hợp đồng.
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request
	MetaData	Bắt buộc	Chứa tham số phụ cần xử lý
	SignedData	Bắt buộc	Dữ liệu dung để ký
	CapicomSignature	Bắt buộc	Chữ ký Capicom
RESPONSE	ResponseCode		Mã trạng thái trả về
	ResponseMessage		Diễn giải mã trạng thái trả về

Thuộc tính		Đặc tính	Diễn giải
	BillCode		BillCode của giao dịch
	SignerInfo		Thông tin chữ ký trong văn bản
	SerialNumber		Định danh chứng thư số
	SubjectName		Tên chứng thư số
	IssuerName		Đơn vị cấp chứng thư số
	DateValid		Ngày có hiệu lực chứng thư số
	DateExpired		Ngày hết hạn chứng thư số

n. SignerAP - Ký file sử dụng SIM PKI - Mode bất đồng bộ

BƯỚC 1: Gửi yêu cầu bao gồm nội dung file cần ký

Request

<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ID>01009090</ID>

<FileType>pdf</FileType>

<MetaData>

<ExternalStorage>P2P</ExternalStorage>

<Method>SignFileRequest</Method>

<VisibleSignature>True</VisibleSignature>

<Coordinate>0,0,200,60</Coordinate>

<PageNo>1</PageNo>

<SignReason>Ký duyệt</SignReason>

<VisualStatus>True</VisualStatus>

<SignatureImage>/9j/4AAQSkZJRgABAQEAYABgAAD/... </SignatureImage>

<MessageMode>Async</MessageMode>

<DisplayMessage>Ma giao dịch {transcode}. Vui lòng xác
nhận</DisplayMessage>

</MetaData>

<WorkerName>SignerAP</WorkerName>

Response

<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ResponseCode>113</ResponseCode>

<ResponseMessage>Request accepted</ResponseMessage>

<TransactionCode>789119</TransactionCode>

<BillCode>TRUSTEDHUB-105442939-20170710091429-251</BillCode>

BƯỚC 2: Thực hiện gọi định kỳ (pooling) để kiểm tra giao dịch đã thành công hay chưa. Mã code 113 thông báo server đã tiếp nhận lệnh thành công. Chú ý, BillCode ở bước 2 được lấy từ Response của bước 1.

Request

<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ID>01009090</ID>

<MetaData>

<Method>SignFileResponse</Method>

<BillCode>TRUSTEDHUB-105442939-20170710091429-251</BillCode>

</MetaData>

<WorkerName>SignerAP</WorkerName>

Response

<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS</ResponseMessage>


<BillCode>TRUSTEDHUB-105442939-20170710091609-252</BillCode>

<SigningCertificate>MIIEoDCCA4igAwIBA...</SigningCertificate>

Nếu như ResponseCode là 116, nghĩa là giao dịch vẫn còn đang được xử lý, tiếp tục thực hiện pooling cho đến khi ResponseCode là 0.

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request

Thuộc tính		Đặc tính	Diễn giải
	FileType	Bắt buộc	Extension của tập tin cần ký
	Method	Bắt buộc	Quy định phương thức cần xử lý <ul style="list-style-type: none"> FileSigningRequest FileSigningStatusRequest
	MessageMode	Bắt buộc	Quy định chế độ gọi <ul style="list-style-type: none"> Async: Đồng bộ Sync: Bất đồng bộ
	DisplayMessage	Bắt buộc	Nội dung hiển thị trên điện thoại của khách hàng để xác nhận giao dịch
	VisibleSignature	Tùy chọn	Tùy chọn hiển thị chữ ký <ul style="list-style-type: none"> True: Hiển thị False: Không hiển thị
	Coordinate	Tùy chọn	Tọa độ hiển thị chữ ký, định dạng X,Y,Z,T <ul style="list-style-type: none"> X: Offset X Y: Offset Y Z: Chiều rộng hình chữ nhật T: Chiều cao hình chữ nhật

Thuộc tính		Đặc tính	Diễn giải
			
	PageNo	Tùy chọn	Trang đặt chữ ký
	SignReason	Tùy chọn	Nội dung ký
	VisualStatus	Tùy chọn	Hiển thị Icon trạng thái chữ ký
	SignatureImage	Tùy chọn	Base64 hình ảnh trong chữ ký. Hỗ trợ định dạng JPG
RESPONSE	ResponseCode		Mã trạng thái trả về
	ResponseMessage		Diễn giải mã trạng thái trả về
	BillCode		BillCode của giao dịch
	SigningCertificate		Chứng thư số của SIM PKI dùng để ký số
	TransactionCode		Mã giao dịch, hiển thị dưới điện thoại người dùng

o. SignatureValidator - Xác thực chữ ký sử dụng worker SignatureValidator

Request

<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ID>01009090</ID>

<WorkerName>SignatureValidator</WorkerName>

<MetaData>

<SignedData>hello</SignedData>

<Encoding>UTF-16LE</Encoding>

<SignatureMethod>TPKI</SignatureMethod>

</MetaData>

<Signature>MIAGCSqG...AAAAA</Signature>

Response

<Channel>TRUSTEDHUB</Channel>

<User>105442939</User>

<ResponseCode>0</ResponseCode>

<ResponseMessage>SUCCESS</ResponseMessage>

<BillCode>TRUSTEDHUB-105442939-20170805224904-1266</BillCode>

<SignerInfos>

<SignerInfo>

<SerialNumber>5404368ce42368e9b42819558ba9d7de</SerialNumber>

<SubjectName>Dương Phương Vũ</SubjectName>

<IssuerName>Mobile-ID Trusted Network</IssuerName>

<DateValid>16/07/2017 13:00:05</DateValid>

<DateExpired>02/04/2037 13:00:05</DateExpired>

<SigningTime>16/07/2017 13:10:08</SigningTime>

</SignerInfo>

</SignerInfos>

Thuộc tính		Đặc tính	Diễn giải
REQUEST	Channel	Bắt buộc	Mã hệ thống Client
	User	Bắt buộc	Định danh khách hàng tại ngân hàng (CIF)
	ID	Tùy chọn	Mã số hợp đồng của hệ thống liên quan
	WorkerName	Bắt buộc	Tên Worker sẽ xử lý request
	SignatureMethod	Bắt buộc	Quy định phương thức cần xử lý. Tùy loại phương thức. Chứng thư số tương ứng sẽ được sử dụng để xác thực <ul style="list-style-type: none"> • TPKE • SPKE • WPKE
	Encoding	Bắt buộc	Encoding của dữ liệu ký <ul style="list-style-type: none"> • UTF-16LE • UTF-8
	SignedData	Bắt buộc	Dữ liệu ký
	Signature	Bắt buộc	Base64 của chữ ký cần xác thực
ESP	ResponseCode		Mã trạng thái trả về

Thuộc tính		Đặc tính	Diễn giải
	ResponseMessage		Diễn giải mã trạng thái trả về
	BillCode		BillCode của giao dịch
	SerialNumber		SerialNumber của CTS ký
	SubjectName		Chủ sở hữu CTS ký
	IssuerName		CA cấp CTS ký
	DateValid		Ngày hiệu lực CTS ký
	DateExpired		Ngày hết hạn CTS ký
	SigningTime		Thời điểm ký

3.2.5. Danh sách các WorkerName được hỗ trợ trong hệ thống

Trong mỗi request gửi lên đều phải có trường <WorkerName></WorkerName>.

Sau đây là danh sách những WorkerName được hỗ trợ trong hệ thống

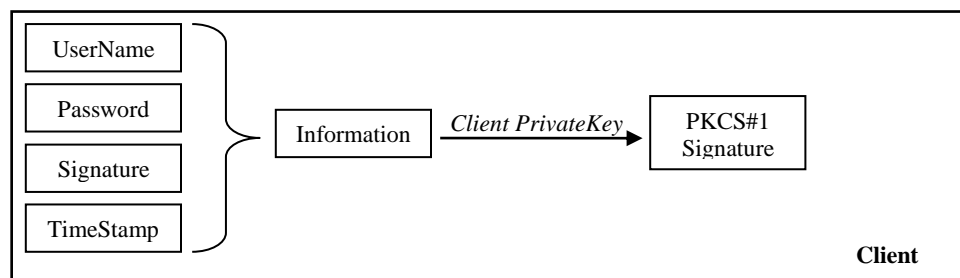
STT	Tên Worker	Mô tả
1	CMSSigner	Ký dữ liệu chuẩn CAPICOM (CMS)
2	PKCS1Signer	Ký dữ liệu chuẩn PKCS#1
3	MultiSigner	Ký văn tổng hợp các loại văn bản
4	DCSigner	Ký file mô hình Distributed Cryptography
5	MultiValidator	Xác thực chữ ký nhiều định dạng file
6	SignatureValidator	Xác thực chữ ký nhiều định dạng (Capicom, PKCS#1)

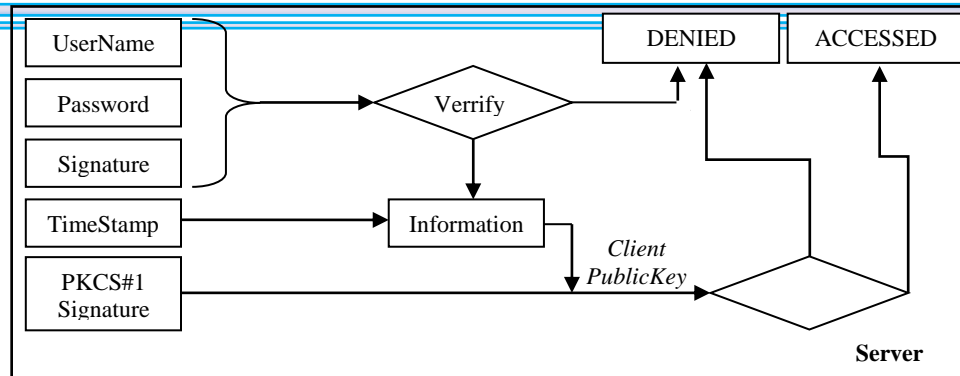
7	GeneralValidator	Xác thực chữ ký nhiều định dạng file không kiểm tra hợp đồng
8	AgreementHandler	Xử lý các tác vụ liên quan đến hợp đồng DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG
9	SignerAP	Worker làm cho TrustedHub đóng vai trò là một AP để tương tác đến dịch vụ MSSP thông qua AE

3.2.6. Thông tin CAGCredential

Đối tượng CAGCredential là 1 thuộc tính của đối tượng TransactionInfo – tham số trong hàm giao tiếp với Client Webservice. Đối tượng này sẽ lưu thông tin định danh và xác thực Client. Thông tin gồm có:

- Username: Tài khoản của Client trên Server
- Password: Mật khẩu tài khoản Client trên Server
- Signature: Chữ ký mẫu của Client đã đăng ký với Server
- Timestamp: Thời gian lần thực hiện tương tác với Server
- PKCS#1 Signature: Dùng PrivateKey của Client để ký thông tin credential





Quy trình xử lý đối tượng CAGCredential ở Client và Server

3.2.7. Cách sử dụng các hàm trong lập trình

❖ Java


```
ClientWSService service = new ClientWSService(new URL("https://Trusted
Hub.com/ClientWS?wsdl")
    , new QName("http://clientws.signserver.org/",
"ClientWSService"));

ClientWS cl = service.getClientWSPort();

String requestXML = "<Channel>Trusted Hub</Channel><User>111488361</User>";

String timestamp = String.valueOf(System.currentTimeMillis());

String username = "Trusted Hub";

String password = "12345678";

String signature = "JVBERi0xLjQKJeLjz9MKMiAwIG9ia...";

String data = username + password + signature + timestamp;

String pkcs1Signature = getDigitalSignature(data);

CagCredential credential = new CagCredential();

credential.setTimestamp(timestamp);

credential.setPassword(password);

credential.setSignature(signature);

credential.setUsername(username);

credential.setPkcs1Signature(pkcs1Signature);

byte[] fileData; // Du lieu tap tin can xu ly

TransactionInfo request = new TransactionInfo();

request.setCredentialData(credential);
```

Cách sử dụng hàm *processData* trong Java

❖ C#

```
string requestXML = "<Channel>Trusted
Hub</Channel><User>111488361</User>";

string timestamp = CurrentTimeMillis().ToString();

string username = "Trusted Hub";

string password = "12345678";

string signature = "JVBERi0xLjQKJeLjz9MKMiAwIG9ia...";

string data = username + password + signature + timestamp;

string pkcs1Signature = getPKCS1Signature(data, "/path/to/client.p12",
"12345678");

cagCredential cag = new cagCredential();

cag.username = username;

cag.password = password;

cag.signature = signature;

cag.timestamp = timestamp;

cag.pkcs1Signature = pkcs1Signature;

ClientWSService service = new ClientWSService("https://Trusted
Hub.com/ClientWS?wsdl");

transactionInfo request = new transactionInfo();

request.credentialData = cag;

request.fileData = getFileToProcess(); // Du lieu tap tin can xu ly

request.xmlData = this.rTBRequest.Text;

processData dataToSend = new processData();
```

Cách sử dụng hàm *processData* trong C#

4. MÔ TẢ GIAO TIẾP VỚI HỆ THỐNG DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG ADMIN WEB SERVICE

Admin Web Service (AdminWS) cung cấp các phương thức dành cho phân hệ quản trị nhằm thực hiện các chức năng sau:

- Cài đặt, thêm mới, xóa, sửa các Worker đảm nhiệm vai trò ký hay xác thực tài liệu.
- Thay đổi địa chỉ IP server, IP filter cho Client.

Địa chỉ Admin Webservice thông thường sẽ là:

<http://<YourIPServer>/DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG/AdminWSService/AdminWS?wsdl>

AdminWS bao gồm các phương thức như sau:

STT	TÊN PHƯƠNG THỨC	THUỘC TÍNH	DIỄN GIẢI
1.	String login	int ClientID String username String password	Đăng nhập vào AdminWS, hàm trả về sessionKey. - ClientID: phân biệt user đăng nhập từ GUI Application hay back-end.
2.	void logout	N/A	Giải phóng session người dùng hiện tại
3.	void activeSigner	int ClientID int signerID String authCode	Kích hoạt Worker - signerID: Id của worker - autCode: Mã PIN để lấy PrivateKey (PKCS#11 hay

STT	TÊN PHƯƠNG THỨC	THUỘC TÍNH	DIỄN GIẢI
		String sessionKey	tập tin PKCS#12) - sessionKey: mã sessionKey trả về từ hàm login
4.	boolean deactivateSigner	int ClientID int signerID String sessionKey	Tạm khóa Worker
5.	void addIpConnect	int ClientID String IP String sessionKey	Thêm địa chỉ IP Client được phép tương tác với AdminWS (không phải tài khoản Admin) và ClientWS - IP: địa chỉ IP
6.	String addWorker	int ClientID String configFile String sessionKey	Thêm 1 Worker - configFile: Tên tập tin chứa thông tin của Worker, tập tin này được lưu cố định trên Server
7.	boolean changeIp	int ClientID String ipAddress String subnetMask String defaultGW String searchDomain String dnsServer String sessionKey	Thay đổi địa chỉ IP của server - ipAddress: địa chỉ IP mới - subnetMask: Subnet Mask mới - defaultGW: Default GateWay mới - searchDomain: searchDomain mới - dnsServer: DNS mới

STT	TÊN PHƯƠNG THỨC	THUỘC TÍNH	DIỄN GIẢI
8.	WSWorkerConfig getCurrentWorkerConfig	int ClientID int workerID String sessionKey	Lấy thông tin cấu hình của một Worker
9.	void setWorkerProperty	int ClientID int workerID String key String value String session	Thêm một giá trị cấu hình cho Worker - key: tên thuộc tính - value: giá trị thuộc tính
10.	boolean removeWorkerProperty	int ClientID int workerID String key String value	Xóa một giá trị cấu hình của Worker
11.	Base64SignerCertReqData getPKCS10CertificateRequestForKey	int ClientID int signerID PKCS10CertReqInfo certReqInfo boolean explicitEccParameters boolean defaultKey String sessionKey	Tạo CSR dựa vào PrivateKey của Worker - certReqInfo: thông tin CSR - defaultKey: sử dụng key mặc định để ký thông tin CSR, ngược lại là trường nextKey

STT	TÊN PHƯƠNG THỨC	THUỘC TÍNH	DIỄN GIẢI
12.	byte[] getSignerCertificate	int ClientID int signerID String sessionKey	Lấy chứng thư mà Worker dùng để ký
13.	List<byte[]> getSignerCertificateChain	int ClientID int signerID String sessionKey	Lấy chứng thư mà Worker dùng để ký và cả chứng thư root của chứng thư ký
14.	Date getSigningValidityNotAfter	int ClientID int workerID String sessionKey	Lấy thông tin hết hạn chứng thư
15.	Date getSigningValidityNotBefore	int ClientID int workerID String sessionKey	Lấy thông tin bắt đầu có hiệu lực của chứng thư
16.	long getKeyUsageCounterValue	int ClientID int workerID String sessionKey	Số lần sử dụng ký của Worker
17.	boolean destroyKey	int ClientID int workerID int purpose String sessionKey	Xóa PrivateKey ra khỏi Worker

STT	TÊN PHƯƠNG THỨC	THUỘC TÍNH	DIỄN GIẢI
18.	String generateSignerKey	int ClientID int workerID String algorithm String keySpec String alias String authCode String sessionKey	Tạo cặp key mới <ul style="list-style-type: none"> - algorithm: Thuật toán Key - keySpec: chiều dài key - alias: định danh key - authCode: Mã PIN của Worker
19.	Collection<KeyTestResult> testKey	int ClientID int workerID String authCode String sessionKey	Kiểm tra hoạt động key của Worker
20.	void uploadSignerCertificate	int ClientID int workerID String signerCert String scope String sessionKey	Cài đặt chứng thư số dùng thẻ ký tài liệu cho Worker <ul style="list-style-type: none"> - signerCert: chứng thư số dạng mã hóa base64
21.	void uploadSignerCertificateChain	int ClientID int workerID String signerCert String scope	Cài đặt chứng thư số dùng để ký kèm theo chứng thư của những CA.

STT	TÊN PHƯƠNG THỨC	THUỘC TÍNH	DIỄN GIẢI
		String sessionKey	
22.	void setGlobalProperty	int ClientID int workerID String key String value String session	Thêm giá trị dùng chung cho toàn hệ thống.
23.	boolean removeGlobalProperty	int ClientID int workerID String key String value String session	Xóa giá trị dùng chung cho toàn hệ thống
24.	List<Integer> getWorkers	int ClientID int workerType String sessionKey	Trả về ID của tất cả các Worker hiện tại - workerType: Loại Worker <ul style="list-style-type: none"> • 1: tất cả Worker • 2: Signer Worker • 3: Service Worker
25.	void rebootServer	int ClientID String sessionKey	Khởi động lại Server
26.	void shutdownServer	int ClientID	Tắt Server

STT	TÊN PHƯƠNG THỨC	THUỘC TÍNH	DIỄN GIẢI
		String sessionKey	
27.	List<String> getAllIpConnect	int ClientID String sessionKey	Trả về danh sách IP được kết nối đến Server
28.	void removeIpConnect	int ClientID String IP String sessionKey	Xóa 1 IP ra khỏi danh sách IP được kết nối đến Server
29.	String reloadWorker	int ClientID int workerID String sessionKey	Tải lại thông tin cấu hình và trạng thái của worker
30.	String removeWorker	int ClientID int workerID String sessionKey	Xóa một Worker
31.	List<AvailableWorkers> getAvailableWorkers	int ClientID String sessionKey	Trả về danh sách Worker hệ thống DỊCH VỤ KÝ SỐ TRÊN THIẾT BỊ DI ĐỘNG cung cấp
32.	String getWorkerConfigFile	int ClientID String configFile String sessionKey	Trả về nội dung của tập tin config Worker
33.	String setWorkerConfigFile	int ClientID	Lưu lại nội dung của tập tin

STT	TÊN PHƯƠNG THỨC	THUỘC TÍNH	DIỄN GIẢI
		String configFile String content String sessionKey	config Worker

-- HẾT --