

HỆ THỐNG MSSP

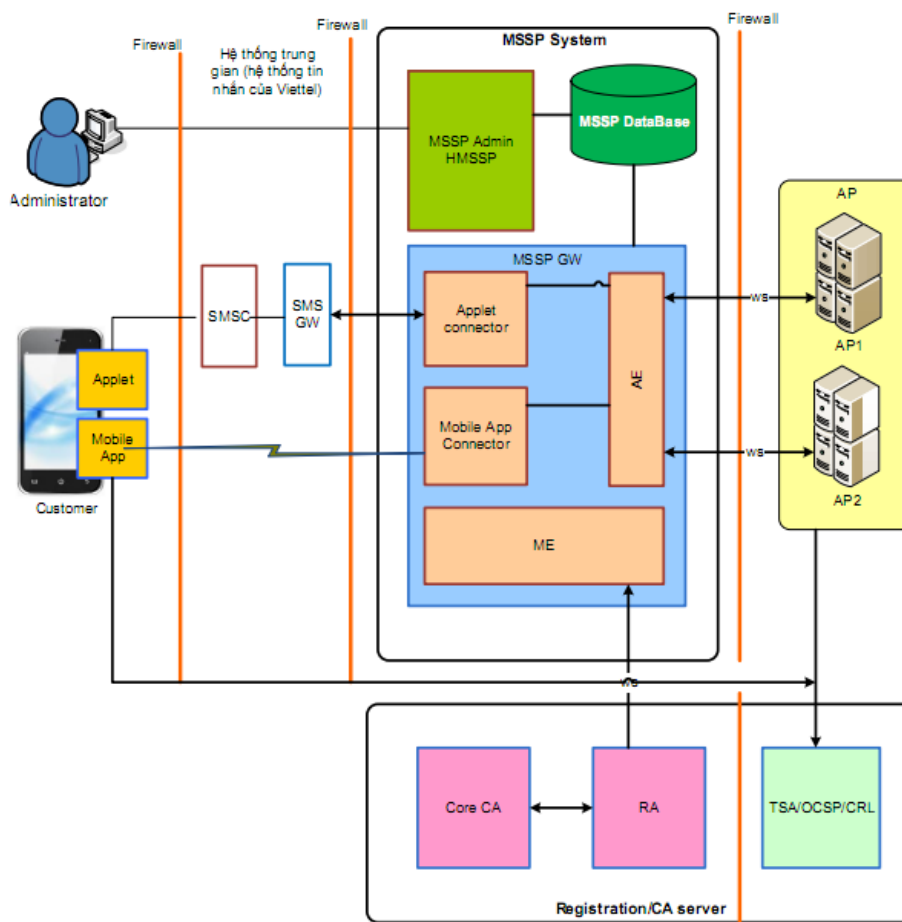
TÀI LIỆU ĐẶC TẢ TÍCH HỢP AE

Tháng 04/2018

Mục lục

1. GIỚI THIỆU	3
2. KÝ SỐ MODE ĐỒNG BỘ	3
2.1. Cấu hình kết nối	3
2.2. Mô tả hàm và các tham số	4
3. KÝ SỐ MODE BẤT ĐỒNG BỘ	4
3.1. Cấu hình kết nối	4
3.2. Mô tả hàm và các tham số	4
4. LẤY THÔNG TIN CHỨNG THƯ SỐ	6
4.1. Cấu hình kết nối	6
4.2. Mô tả hàm và các tham số	6
5. DANH MỤC MÃ LỖI (EXCEPTION CODE)	6

1. GIỚI THIỆU



MSSP Gateway (**MSSP GW**): Là hệ thống trung tâm đảm bảo các giao tiếp với các AP, SMSC và thiết bị đầu cuối của khách hàng. Gồm các connector như sau:

- AE: Cung cấp Webservice: yêu cầu ký, hủy ký, tra cứu...

Thông tin dịch vụ MSSP của Ban Cơ yếu Chính phủ:

- Đường dẫn dịch vụ:
https://mpki.ca.gov.vn:18083/soap/services/MSS_SignaturePort
- Giao thức kết nối TLSv1.2 xác thực hai chiều

Khi cơ quan, đơn vị có yêu cầu tích hợp hệ thống MSSP của Ban Cơ yếu Chính phủ, sẽ được cấp một định danh APIP và chứng thư số máy khách để có thể kết nối đến dịch vụ.

2. KÝ SỐ MODE ĐỒNG BỘ

2.1. Cấu hình kết nối

Thông tin kết nối lưu ở file **conf/examples.conf** của project. Chi tiết như sau:

ssl.truststore.file	Đường dẫn đến file truststore
ssl.truststore.password	Mật khẩu của file truststore
ssl.keystore.file	Đường dẫn đến file keystore
ssl.keystore.password	Mật khẩu của file keystore
ssl.keystore.type	Loại file keystore

ap.id	Định danh của AP
ap.password	Mật khẩu của AP
mssp.id	Định danh của hệ thống MSSP
mssp.signature.url	Đường dẫn Service yêu cầu chữ ký số
mssp.status.url	Đường dẫn Service truy vấn yêu cầu
mssp.receipt.url	Đường dẫn Service truy vấn lịch sử giao dịch
mssp.profile.url	Đường dẫn Service truy vấn profile chữ ký số

2.2. Mô tả hàm và các tham số

```
MSS_SignatureReqType sigReq =
etsiClient.createSignatureRequest(

    apTransId,

    msisdn,

    dataToBeSigned,

    dataToBeDisplayed,

    signatureProfile,

    mssFormat,

    messagingMode);
```

Tham số	Kiểu dữ liệu	Mô tả
apTransId	String	Transaction ID của giao dịch
msisdn	String	Số điện thoại
dataToBeSigned	DTBS	Dữ liệu ký
dataToBeDisplayed	String	Thông tin giao dịch hiển thị dưới điện thoại của khách hàng
signatureProfile	String	Profile của chữ ký số
mssFormat	String	Định dạng chữ ký số:
messagingMode	MessagingModeType	Mode giao dịch. Đối với trường hợp đồng bộ thì messagingMode = MessagingModeType.synch

3. KÝ SỐ MODE BẤT ĐỒNG BỘ

3.1. Cấu hình kết nối

Tương tự như mục 2.1

3.2. Mô tả hàm và các tham số

3.2.1. Yêu cầu chữ ký số

```

MSS_SignatureReqType sigReq =
etsiClient.createSignatureRequest(

    apTransId,

    msisdn,

    dataToBeSigned,

    dataToBeDisplayed,

    signatureProfile,

    mssFormat,

    messagingMode);

```

Tham số	Kiểu dữ liệu	Mô tả
apTransId	String	Transaction ID của giao dịch
msisdn	String	Số điện thoại
dataToBeSigned	DTBS	Dữ liệu ký
dataToBeDisplayed	String	Thông tin giao dịch hiển thị dưới điện thoại của khách hàng
signatureProfile	String	Profile của chữ ký số
mssFormat	String	Định dạng chữ ký số:
messagingMode	MessagingModeType	Mode giao dịch. Đối với trường hợp bất đồng bộ thì messagingMode = MessagingModeType. asynchClientServer

Lưu ý: Trường hợp bất đồng bộ, bước này sẽ trả về TransactionID của giao dịch. TransactionID sẽ được sử dụng ở bước kiểm tra yêu cầu chữ ký số.

3.2.2. Kiểm tra yêu cầu chữ ký số

```

MSS_SignatureRespType sigResp = new MSS_SignatureRespType();
sigResp.setAP_Info(apInfo);
sigResp.setMSSP_Info(msspInfo);
sigResp.setMSSP_TransID(new NCName("M1798702590996149"));

MSS_StatusReqType statusReq = etsiClient.createStatusRequest(

    sigResp,

    apTransId);

```

Tham số	Kiểu dữ liệu	Mô tả
sigResp	MSS_SignatureRespType	Tạo lại thông tin yêu cầu. Object này bao gồm TransactionID của bước yêu cầu chữ ký số
apTransId	String	Transaction ID của giao dịch

4. LẤY THÔNG TIN CHỨNG THƯ SỐ

4.1. Cấu hình kết nối

Tương tự như mục 2.1

4.2. Mô tả hàm và các tham số

```
MSS_RegistrationReqType registrationReq =
etsiClient.createRegistrationRequest(

    apTransId,

    msisdn,

    signatureProfile);
```

Tham số	Kiểu dữ liệu	Mô tả
apTransId	String	Transaction ID của giao dịch
msisdn	String	Số điện thoại
signatureProfile	String	Profile của chữ ký số: <ul style="list-style-type: none"> http://mobile-id.vn/digitalSignature http://mobile-id.vn/authentication

5. DANH MỤC MÃ LỖI (EXCEPTION CODE)

101	WRONG_PARAM
102	MISSING_PARAM
103	WRONG_DATA_LENGTH
104	UNAUTHORIZED_ACCESS
105	UNKNOWN_CLIENT
106	HANDSHAKE_REQUIRED
107	INAPPROPRIATE_DATA
108	INCOMPATIBLE_INTERFACE
109	UNSUPPORTED_PROFILE
208	EXPIRED_TRANSACTION
209	OTA_ERROR
401	USER_CANCEL
402	PIN_NR_BLOCKED
403	CARD_BLOCKED
404	NO_KEY_FOUND
405	NO_URL_FOUND
406	PB_SIGNATURE_PROCESS
407	REGISTRATION_NOK
422	NO_CERT_FOUND
423	CRL_PB

424	CRL_EXPIRED
425	ERROR_CERTIFICATE
900	INTERNAL_ERROR