**TÀI LIỆU MÔ TẢ SIGNPLUGINv2.2**

1. Yêu cầu:

* Hỗ trợ https://127.0.0.1:14408 và http://127.0.0.1:14008 (PORT riêng cho FPTCA)

1. Các chức năng
   1. getSession

* Sử dụng để lấy thông tin session, mối session có giá trị trong vòng 30 phút
* Input: định dạng base64 của chuỗi json gồm:
  + OperationId : 1
  + pkcs11Lib: Danh sách tên thư viện PKCS#11 (Tùy Chọn)
* Output: Trả về base64 của chuỗi json gồm:
  + ResponseCode
  + ResponseMsg
  + OperationId
  + SessionId

ResponseCode = 0 là thành công, còn lại là lỗi, chi tiết lỗi trong ResponseMsg. SessionId được sử dụng để gọi các chức năng còn lại của SignPlugin

* 1. getCertificate
* Sử dụng để chọn và lấy thông tin chứng thư số (CTS) cần để đăng ký hoặc ký
* Input: định dạng base64 của chuỗi json gồm:
  + OperationId : 2
  + SessionId : là giá trị nhận được trong chức năng getSession
  + checkOCSP : Tùy chọn kiểm tra OCSP của chứng thư số. mặc định không kiểm tra (giá trị: 1 - Kiểm tra OCSP,0 - Không kiểm tra OCSP) (Tùy chọn)
  + timeServer : Thời gian của server để kiểm tra tính hợp lệ của CTS, nếu không truyền thì mặc định lấy thời gian local trên máy tính Khách Hàng. Định dạng: YYYYmmddhhmmss (Tùy chọn)
* Output: Trả về base64 của chuỗi json gồm:
  + ResponseCode
  + ResponseMsg
  + OperationId
  + SessionId
  + certInfo:
    - CommonName :Thông tin chủ thể của chứng thư số
    - SerialNumber :Chuỗi serialnumber của chứng thư số
    - Issuer :Thông tin CA cấp chứng thư số
    - NotBefore :Thời gian có hiệu lực của chứng thư số
    - NotAfter :Thời gian hết hạn của chứng thư số
    - SubjectDN :Thông tin liên quan tới chủ thể của chứng thư số
    - Base64Encode :Thông tin định dạng base64 của chứng thư số
    - Thumbprint :Thumprint của chứng thư số

ResponseCode = 0 là thành công, còn lại là lỗi, chi tiết lỗi trong ResponseMsg

* 1. Sign
* Sử dụng để ký dữ liệu
* Input: định dạng base64 của chuỗi json gồm:
  + OperationId : 3
  + SessionId : là giá trị nhận được trong chức năng getSession
  + checkOCSP : Tùy chọn kiểm tra OCSP của chứng thư số. mặc định không kiểm tra (giá trị: 1 - Kiểm tra OCSP,0 - Không kiểm tra OCSP) (Tùy chọn)
  + timeServer : Thời gian của server để kiểm tra tính hợp lệ của CTS, nếu không truyền thì mặc định lấy thời gian local trên máy tính Khách Hàng. Định dạng: YYYYmmddhhmmss(Tùy chọn)
  + DataToBeSign :Base64 của dữ liệu cần ký
  + sigLevel: Level của CAdES (CADES-BES| CADES-T| CADES-C| CADES-X1| CADES-X2| CADES-XL1| CADES-XL2). Mặc định CADES-BES (Tùy chọn)
  + urlTimestamp: URL của TimeStamp (Áp dụng trong trường hợp ký nhãn thời gan và sigLevel >= CADES-T) (Tùy chọn)
  + reqDigest: giá trị 1 - Yêu cầu băm dữ liệu hoặc 0 - không yêu cầu băm dữ liệu (Trong trường hợp dữ liệu đã được băm trước đó) (Tùy chọn)
  + algDigest: Thuật toán băm dữ liệu (MD5| SHA\_1| SHA\_224| SHA\_256| SHA\_384| SHA\_512). Mặc định SHA\_1 (Chỉ hỗ trợ MD5| SHA\_1| SHA\_256) (Tùy chọn)
* Output: Trả về base64 của chuỗi json gồm:
  + ResponseCode
  + ResponseMsg
  + OperationId :3
  + SessionId
  + Signature :Định dạng chữ ký CAPICOM (PKCS#7)

ResponseCode = 0 là thành công, còn lại là lỗi, chi tiết lỗi trong ResponseMsg

* 1. Verify
* Sử dụng để xác thực tính hợp lệ của chữ ký
* Input: định dạng base64 của chuỗi json gồm:
  + OperationId : 4
  + SessionId : là giá trị nhận được trong chức năng getSession
  + DataToBeSign :Base64 của dữ liệu cần ký
  + signature :Định dạng chữ ký CAPICOM (PKCS#7)
  + ~~signAttached: 1 - Chữ ký Attached; 0 - Chữ ký Detached (Tùy chọn)~~
* Output: Trả về base64 của chuỗi json gồm:
  + ResponseCode
  + ResponseMsg
  + OperationId
  + SessionId
  + DataToBeSign :Base64 của dữ liệu ký
  + SingerInfo:
    - CommonName :Thông tin chủ thể của chứng thư số
    - SerialNumber :Chuỗi serialnumber của chứng thư số
    - Issuer :Thông tin CA cấp chứng thư số
    - NotBefore :Thời gian có hiệu lực của chứng thư số
    - NotAfter :Thời gian hết hạn của chứng thư số
    - SubjectDN :Thông tin liên quan tới chủ thể của chứng thư số
    - Base64Encode :Thông tin định dạng base64 của chứng thư số
    - Thumbprint :Thumprint của chứng thư số

ResponseCode = 0 là chữ ký hợp lệ, còn lại là chữ ký không hợp lệ hoặc lỗi, chi tiết lỗi trong ResponseMsg

* 1. DCSigner
* Sử dụng để ký chữ ký định dạng PKCS#1
* Input: định dạng base64 của chuỗi json gồm:
  + OperationId : 5
  + SessionId : là giá trị nhận được trong chức năng getSession
  + DataToBeSign :Base64 của dữ liệu cần ký
  + checkOCSP : Tùy chọn kiểm tra OCSP của chứng thư số. mặc định không kiểm tra (giá trị: 1 - Kiểm tra OCSP,0 - Không kiểm tra OCSP) (Tùy chọn)
  + reqDigest: giá trị 1 - Yêu cầu băm dữ liệu hoặc 0 - không yêu cầu băm dữ liệu (Trong trường hợp dữ liệu đã được băm trước đó) (Tùy chọn)
  + algDigest: Thuật toán băm dữ liệu (MD5| SHA\_1| SHA\_224| SHA\_256| SHA\_384| SHA\_512). Mặc định SHA\_1 (Chỉ hỗ trợ MD5| SHA\_1| SHA\_256)(Tùy chọn)
* Output: Trả về base64 của chuỗi json gồm:
  + ResponseCode
  + ResponseMsg
  + OperationId
  + SessionId
  + Signature: Chữ ký định dạng KCS#1
  + DataToBeSign :Base64 của dữ liệu ký
  + certInfo:
    - CommonName :Thông tin chủ thể của chứng thư số
    - SerialNumber :Chuỗi serialnumber của chứng thư số
    - Issuer :Thông tin CA cấp chứng thư số
    - NotBefore :Thời gian có hiệu lực của chứng thư số
    - NotAfter :Thời gian hết hạn của chứng thư số
    - SubjectDN :Thông tin liên quan tới chủ thể của chứng thư số
    - Base64Encode :Thông tin định dạng base64 của chứng thư số
    - Thumbprint :Thumprint của chứng thư số
  + TimeStamping: Thời gian ký, định dạng yyyyMMddhhmmss

ResponseCode = 0 là thành công, còn lại là lỗi, chi tiết lỗi trong ResponseMsg

* 1. BrowseFile
* Sử dụng để lấy đường dẫn file cần mở hoặc cần lưu
* Input: định dạng base64 của chuỗi json gồm:
  + OperationId : 6
  + SessionId : là giá trị nhận được trong chức năng getSession
  + openFile: giá trị: 1- chọn đường dẫn file cần mở, 0 - chọn đường dẫn file cần lưu file. Mặc định là 1
* Output: Trả về base64 của chuỗi json gồm:
  + ResponseCode
  + ResponseMsg
  + OperationId
  + SessionId
  + PathFile: Đường dẫn file cần mở hoặc cần lưu

ResponseCode = 0 là thành công, còn lại là lỗi, chi tiết lỗi trong ResponseMsg

* 1. SignFile
* Sử dụng để ký file PDF, Office, XML
* Input: định dạng base64 của chuỗi json gồm:
  + OperationId : 7
  + SessionId : là giá trị nhận được trong chức năng getSession
  + checkOCSP : Tùy chọn kiểm tra OCSP của chứng thư số. mặc định không kiểm tra (giá trị: 1 - Kiểm tra OCSP,0 - Không kiểm tra OCSP) (Tùy chọn)
  + infile: Đường dẫn file cần ký
  + outfile: Đường dẫn file đã ký
  + algDigest: Thuật toán băm dữ liệu (MD5| SHA\_1| SHA\_224| SHA\_256| SHA\_384| SHA\_512). Mặc định SHA\_1 (Tùy chọn)
  + invisible: giá trị: 1 - không hiện khung chữ ký trên file, 0 - hiện khung chữ ký trên file (Chỉ áp dụng cho PDF) (Tùy chọn)
  + signerTitle: Tiêu đề tên người ký (chỉ có tác dụng trong trường hợp invisible = 0). Mặc đinh: "KÝ BỞI:" (Chỉ áp dụng cho PDF) (Tùy chọn)
  + signTimeTitle: Tiêu đề thời gian ký (chỉ có tác dụng trong trường hợp invisible = 0). Mặc đinh: "KÝ NGÀY:" (Chỉ áp dụng cho PDF) (Tùy chọn)
  + pageIndex: Vị trí trang đặt chữ ký (chỉ có tác dụng trong trường hợp invisible = 0). Mặc định: đặt ở trang cuối cùng của tài liệu (Chỉ áp dụng cho PDF) (Tùy chọn)
  + offsetX, offsetY, sigWidth, sigHeight: Tọa độ và kích thước khung chữ ký (chỉ có tác dụng trong trường hợp invisible = 0) (Chỉ áp dụng cho PDF) (Tùy chọn)
  + logoPath: Đường dẫn file hình ảnh nền chữ ký (chỉ có tác dụng trong trường hợp invisible = 0) (Chỉ áp dụng cho PDF) (Tùy chọn)
  + xades\_Form: giá trị (XADES\_T| ~~XADES\_C| XADES\_X| XADES\_X\_L| XADES\_A~~) chỉ áp dụng cho Office và XML (Mặc định và chỉ hỗ trợ XADES\_T) (Tùy chọn)
  + xades\_Version: giá trị (XADES\_v1\_1\_1| XADES\_v1\_2\_2| XADES\_v1\_3\_2| XADES\_v1\_4\_1). Mặc định: XADES\_v1\_4\_1 (Chỉ áp dụng cho XML) (Tùy chọn)
  + tagXML: giá trị "\*" ký cho cả tài liệu XML, Trường hợp khác chỉ định tên tag XML cần ký (Chỉ áp dụng cho XML) (Tùy chọn)
  + XMLDSig : giá trị: 1 - chữ ký định dạng XMLDSig; 0 - chữ ký định dạng XMLXAdES. Mặc định 1 (Chỉ áp dụng cho XML) (Tùy chọn)
* Output: Trả về base64 của chuỗi json gồm:
  + ResponseCode
  + ResponseMsg
  + OperationId
  + SessionId
  + PathFile: Đường dẫn file sau khi ký

ResponseCode = 0 là thành công, còn lại là lỗi, chi tiết lỗi trong ResponseMsg

* 1. SignXML
* Sử dụng để ký dữ liệu file XML
* Input: định dạng base64 của chuỗi json gồm:
  + OperationId : 8
  + SessionId : là giá trị nhận được trong chức năng getSession
  + checkOCSP : Tùy chọn kiểm tra OCSP của chứng thư số. mặc định không kiểm tra (giá trị: 1 - Kiểm tra OCSP,0 - Không kiểm tra OCSP) (Tùy chọn)
  + DataToBeSign :Base64 của dữ liệu XML cần ký
  + algDigest: Thuật toán băm dữ liệu (MD5| SHA\_1| SHA\_224| SHA\_256| SHA\_384| SHA\_512). Mặc định SHA\_1 (Chỉ hỗ trợ MD5| SHA\_1| SHA\_256)(Tùy chọn)
  + xades\_Form: giá trị (XADES\_T| ~~XADES\_C| XADES\_X| XADES\_X\_L| XADES\_A~~)(Mặc định và chỉ hỗ trợ XADES\_T) (Tùy chọn)
  + xades\_Version giá trị (XADES\_v1\_1\_1| XADES\_v1\_2\_2| XADES\_v1\_3\_2| XADES\_v1\_4\_1). Mặc định: XADES\_v1\_4\_1 (Tùy chọn)
  + tagXML: giá trị "\*" ký cho cả tài liệu XML, Trường hợp khác chỉ định tên tag XML cần ký (Tùy chọn)
  + XMLDSig : giá trị: 1 - chữ ký định dạng XMLDSig; 0 - chữ ký định dạng XMLXAdES. Mặc định 1(Tùy chọn)
  + sigId: Thiết lập giá trị Id cho chữ ký (Tùy chọn)
* Output: Trả về base64 của chuỗi json gồm:
  + ResponseCode
  + ResponseMsg
  + OperationId
  + SessionId
  + Base64Result: Base64 của dữ liệu XML sau khi ký

ResponseCode = 0 là thành công, còn lại là lỗi, chi tiết lỗi trong ResponseMsg

1. Thông tin mã lỗi

* 0 - Success
* 1 - Invalid input format. Require base64 of JSON
* 2 - Invalid OperationId
* 3 - Invalid PKCS#11 library or not support
* 4 - Error during load PKCS#11 library
* 5 - Error connect with Token
* 6 - The trial version has expired
* 7 - Invalid session
* 8 - User cancel or certificate not found
* 9 - Invalid certificate
* 10 - Error during check OCSP or certificate was revoked
* 11 - Not support certificate
* 12 - Invalid time format. Request format: YYYYmmddhhmmss
* 13 - Error during parser certificate
* 14 - Invalid signature
* 15 - Out of memory
* 16 - Error during calculate digest
* 17 - Error during sign digest
* 18 - Error during genearate signature
* 19 - User cancel or file not found
* 20 - Invalid file type
* 21 - Error during read file
* 22 - The document is encrypted and cannot be signed
* 23 - Cannot sign document
* 24 - Error during write file
* 25 - Error load XML data
* 26 - Timestamp URL is not set
* 27 - Unsupport signature level
* 28 - Unsupport XAdES FORM
* 29 - Unsupport XAdES Version

1. History

* Future
* 04-06-2018
  + Input parameter (old -> new):
    - operationId -> OperationId
    - sessionId -> SessionId
    - base64DTBS -> DataToBeSign
    - xmlDSig -> XMLDSig
  + Output parameter (old -> new):
    - CertInfo -> certInfo
    - base64DTBS -> DataToBeSign
* 22-10-2018
  + Input parameter:
    - Thêm sigId (SignXML)
    - Thêm extFile, logoData (SignBinDoc)
  + Thêm function SignBinDoc