# GIẢI PHÁP TÍCH HỢP VNPT-CA PLUGIN

**Hà Nội, 03– 2017**

# MỤC LỤC

# 1. GIỚI THIỆU

## 1.1. Mục đích

Tài liệu mô tả giải pháp tích hợp VNPT-CA Plugin (plugin) vào hệ thống ứng dụng nền web của khách hàng, giải quyết vấn đề ký số cho các ứng dụng nền web.

Plugin là ứng dụng bổ sung tính năng ký số cho trình duyệt. Plugin cung cấp các chức năng ký dự liệu Xml, Pdf, Office, Cms, các chức năng được cung cấp dưới dạng api. Ứng dụng web có thể sử dụng các chức năng của plugin thông qua javascript.

## 1.2. Thuật ngữ và từ viết tắt

| | |
|---|---|
| VNPT-CA | Chứng thư số do VNPT-CA cấp phát |
| VNPT-CA Plugin | Ứng dụng bổ sung tính năng ký số cho ứng dụng web |
| CTDT | Phòng giải pháp chứng thực điện tử |
| KH | Khách hàng |
| CTS | Chứng thư số |
| CA | Certificate Authority – Nhà cung cấp chứng thư số |
| CRL | Certificate Revocation List |
| OCSP | Online Certificate Status Protocol |

# 2. NHU CẦU TÍCH HỢP CHỮ KÝ SỐ

## 2.1. Khảo sát hệ thống

Hầu hết các ứng dụng web của doanh nghiệp hiện nay đều được phát triển dựa trên một số công nghệ sau:

- Window form client-server
- ASP .Net
- Java web based Application
- PHP web based Application

Các hệ thống ứng dụng thường phục vụ cho công việc điều hành văn bản, giao dịch với khách hàng, giao dịch bằng email.

Để đảm bảo an ninh thông tin, các hệ thống thường áp dụng các công nghệ bảo mật:

- Login bằng user/pass, otp.
- Sử dụng các firewall, các thiết bị bảo vệ mạng.
- Sử dụng các kĩ thuật về lập trình để bảo vệ mã nguồn ứng dụng.

Các giải pháp này phần lớn là bảo vệ mang tính phòng ngự. Khi tăng cường an ninh thì hệ thống buộc phải giảm khả năng trao đổi thông tin. Điều này là không phù hợp với tình hình toàn cầu hóa thông tin như hiện nay. Với giải pháp sử dụng công nghệ hạ tầng khóa công khai PKI, hệ thống vừa được bảo vệ, lại vừa có khả năng trao đổi thông tin hai chiều hoàn toàn bảo mật.

Dưới đây là một số khả năng của hệ thống khi áp dụng PKI:

- Mã hóa thông tin hai chiều SSL.
- Xác thực người dùng đăng nhập bằng chứng thư số, chữ kí số.
- Đảm bảo dữ liệu tin cậy, chính xác (toàn vẹn dữ liệu).
- Tăng cường khả năng ghi log làm bằng chứng thông tin.
- Đảm bảo khả năng sẵn sàng của hệ thống.

### 2.2. Các bước thực hiện điển hình

- ***Bước 1***: Ứng dụng web của khách hàng tạo ra dữ liệu
- ***Bước 2***: Người dùng thực hiện ký số lên dữ liệu được sinh ra tại bước 1.
- ***Bước 3***: Sau khi người dùng đã ký xong thì hệ thống sẽ xác thực lại các dữ liệu đã ký, kiểm tra tính hợp lệ của chữ ký, trạng thái chứng thư, tính toàn vẹn của dữ liệu.
- ***Bước 4***: Hệ thống lưu thông tin và chuyển sang các tiến trình tiếp theo.

## 3. GIẢI PHÁP TÍCH HỢP VNPT – CA PLUGIN

### 3.1. Mô tả

VNPT-CA Plugin (plugin) có độ an toàn và bảo mật cao.

Plugin của VNPT-CA không sử dụng các công nghệ cũ như Applet, NPAPI, ActiveX. Các công nghệ cũ này đã được chỉ ra các lỗi lỗ hổng bảo mật. Các trình duyệt phổ biến hiện nay đã ngừng hỗ trợ các công nghệ cũ này trên các phiên bản trình duyệt mới nhất. Google Chrome đã loại bỏ NPAPI từ tháng 9 năm 2015, Firefox phiên bản 52 trở lên đã loại bỏ NPAPI, Microsoft Edge đã ngừng hỗ trợ ActiveX.

Plugin của VNPT-CA sử dụng công nghệ mới tương thích với các phiên bản mới nhất của các trình duyệt phổ biến nhất hiện nay như Google Chrome, Firefox, Internet Explorer, Microsoft Edge,…

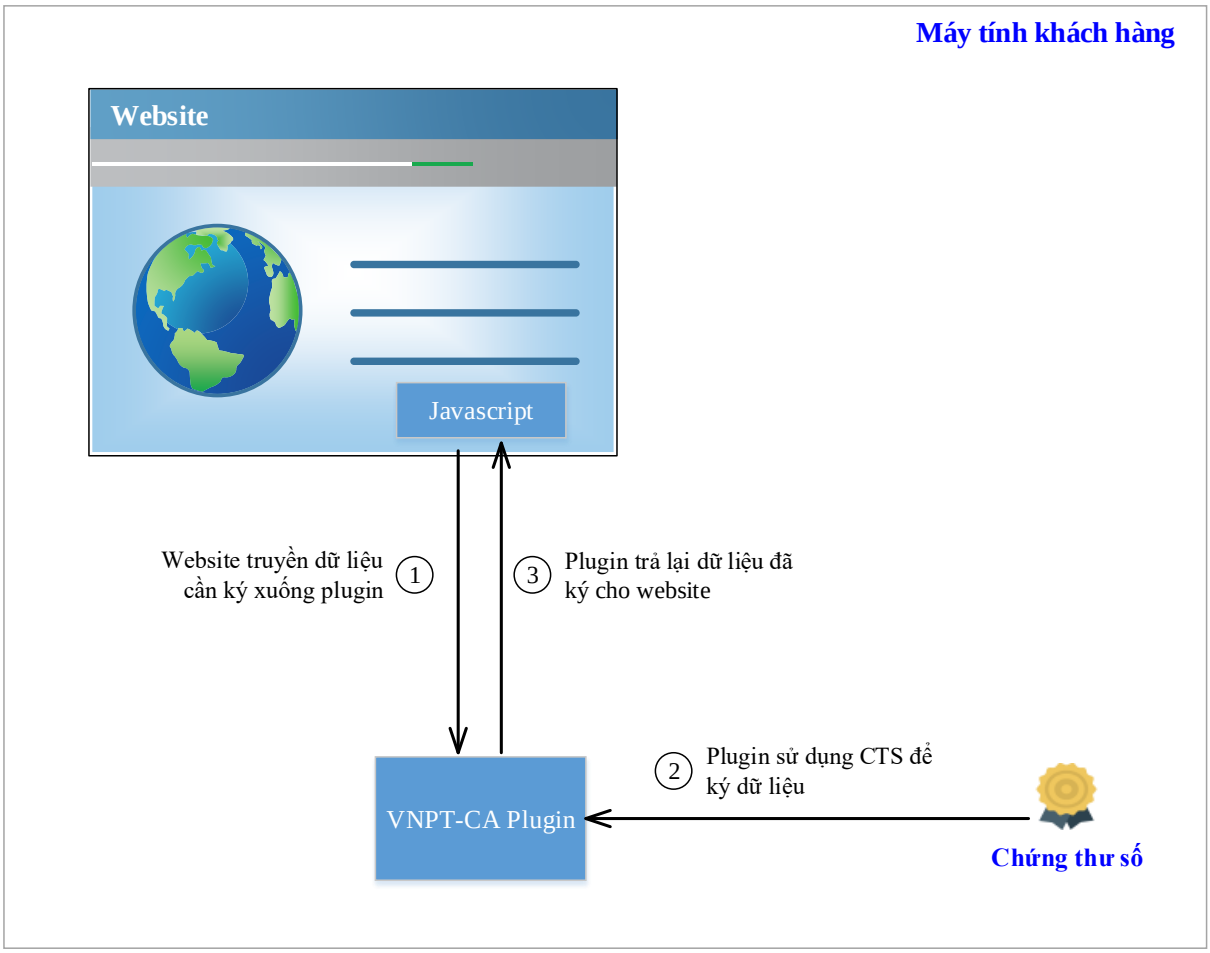
**Mô hình ký số tích hợp plugin vào các ứng dụng web**

- Sử dụng plugin và javascript: javascript sẽ gọi các api do plugin cung cấp để thực hiện ký dữ liệu.
- Plugin thực hiện ký số trên dữ liệu do website truyền xuống.
- Quá trình đóng gói, ký dữ liệu được thực hiện ngay tại client.

**Mô tả chức năng plugin**

- Tích hợp vào website, cho phép website thực hiện ký số lên các dữ liệu (Pdf, Xml, Excel, Word, Power Point, Text).
- Cho phép website lấy thông tin của chứng thư số trên máy người dùng.
- Cho phép website kiểm tra được hiệu lực của chứng thư số của người dùng, thông qua các giao thức OCSP, CRL
- Các tiện ích khác: chọn file, hiển thị thông tin chi tiết của chứng thư,…

## 3.2. Mô hình tổng quan




**Thành phần**

- **Website:** là website có nhu cầu tích hợp ký số của khách hàng
- **Javascript:** thư viện javascript được tích hợp trên website của khách hàng
- **VNPT-CA Plugin:** là phần mềm bổ sung tính năng ký số cho trình duyệt, được cài đặt trên máy người dùng.
- **Chứng thư số:** chứng thư số được lưu trong Usb Token, chứng thư số mềm,…

**Luồng xử lý**

- Bước 1: Người dùng thực hiện ký dữ liệu trên website, website truyền dữ liệu cần ký xuống Plugin.
- Bước 2: Plugin sử dụng CTS của khách hàng để ký lên dữ liệu.
- Bước 3: Plugin trả lại dữ liệu đã ký cho website.

## 3.3. Đánh giá

- Giải pháp này phù hợp với các hệ thống có sẵn tại cơ quan tổ chức doanh nghiệp, ứng dụng mang tính công cộng, sử dụng nhiều chữ ký số cá nhân.
- Hệ thống triển khai tiện lợi, đơn giản hóa quá trình ký số của người dùng.
- Hệ thống tương thích với tất cả các trình duyệt khác nhau

- Hệ thống ký số với tất cả chữ ký số của các nhà cung cấp được cấp phép của Bộ Thông tin và Truyền thông.

## 4. THÔNG SỐ KỸ THUẬT

### 4.1. Hệ điều hành và trình duyệt

- **Hệ điều hành**:
  - Hỗ trợ hệ điều hành Windows phiên bản XP SP3 trở lên.
  - Hỗ trợ hệ điều hành MAC
- **Trình duyệt**: hỗ trợ các trình duyệt sau
  - Microsoft Internet Explorer (IE) phiên bản 11
  - Microsoft Edge phiên bản 16 trở lên
  - Mozila Firefox phiên bản 50 trở lên
  - Google Chrome phiên bản 53 trở lên
  - Cốc cốc phiên bản 53 trở lên
  - Safari phiên bản 9 trở lên

### 4.2. Phương án cập nhật

Quá trình cập nhật phiên bản mới của plugin được chia làm hai phần:

- Cập nhật phần mềm plugin được cài đặt trên máy người dùng
- Cập nhật thư viện javascript tích hợp trên website

Các trường hợp cần cập nhật plugin

- **Cập nhật chức năng mới**
  - Cập nhật phần mềm plugin: phần mềm tự động cập nhật lên phiên bản mới.
  - Cập nhật thư viện javascript: website tích hợp cập nhật thư viện javascript lên phiên bản mới. Phần cập nhật này không bắt buộc.
  - Việc cập nhật plugin lên phiên bản mới không gây ảnh hưởng tới các chức năng đang sử dụng trên các website.
- **Xử lý sự cố:** sự cố có thể xảy ra trong trường hợp một chức năng nào đó của plugin chạy lỗi hoặc trình duyệt cập nhật phiên bản mới gây ảnh hưởng tới hoạt động của plugin,… Phương án cập nhật gồm các phần sau:
  - Cập nhật phần mềm plugin: phần mềm tự động cập nhật lên phiên bản mới.
  - Cập nhật thư việc javascript: phần cập nhật này tùy từng trường hợp cụ thể sẽ cần cập nhật hay không?

## 5. HƯỚNG DẪN TÍCH HỢP

### 5.1. Hướng dẫn tích hợp

Tích hợp plugin gồm hai phần: bộ cài đặt VNPT-CA Plugin_Setup.exe trên máy client và tích hợp thư viện javascript vnpt-plugin.js trên website.

- Chạy bộ cài đặt VNPT-CA Plugin_Setup.exe trên máy client: cài đặt như các phần mềm thông thường.
- Tích hợp thư viện javascript trên website: nhúng thư viện vnpt-plugin.js do VNPT-CA cung cấp vào website tích hợp.

## 5.2. Hương dẫn sử dụng các chức năng

### *5.2.1. Mô tả cách thức hoạt động của plugin*

Sau khi đã nhúng file thư viện vnpt-plugin.js vào website tích hợp, bạn chỉ cần sử dụng đối tượng vnpt-plugin để gọi các hàm plugin cung cấp.

Plugin hoạt động theo cơ chế bất đồng bộ. Website gọi, truyền dữ liệu xuống plugin thông qua các hàm javascript, website nhận lại kết quả từ plugin bằng cách sử dụng hàm javascript callback. Plugin sau khi xử lý xong, sẽ tự động gọi lại hàm javascript callback để trả lại kết quả cho website. Xem thêm trong phần ví dụ tích hợp.

Cơ chế gửi nhận bất đồng bộ giúp cho trình duyệt không gặp hiện tượng "Not responding".

### *5.2.2. Mô tả các hàm plugin cung cấp*

#### 5.2.2.1. vnpt_plugin

**a. Mô tả**

Đây là đối tượng javascript cung cấp các hàm chức năng của plugin.

**b. Phương thức**

- signXML: function (data, funcCallback, xmlSigner)
  - Chức năng: ký dữ liệu xml
  - Tham số
    - data: dữ liệu cần ký. Dữ liệu cần ký được mã hóa base64
    - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
    - xmlSigner: tham số cấu hình chữ ký xml. Xem thêm mục 4.2.2.2.
  - Kết quả: kết quả trả về là chuỗi json với định dạng như sau

    "\"code\":{0}, \"data\":\"{1}\", \"error\":\"{2}\""

    Trong đó các trường có ý nghĩa như sau:

    - code: mã trả về. Giá trị và ý nghĩa tương ứng như sau:
      - 0: ký thành công
      - 1: dữ liệu đầu vào rỗng hoặc không đúng định dạng
      - 2: không tìm thấy chứng thư số
      - 3: ký thất bại
      - 4: không tìm thấy private key
      - 5: nguyên nhân không xác định
      - 8: không tìm thấy thẻ ký số
      - 9: không tham chiếu được tới id thẻ ký số
      - 10: dữ liệu đầu vào chứa một hoặc nhiều chữ ký không hợp lệ
      - 11: người dùng hủy bỏ
    - data: dữ liệu đã ký trong trường hợp ký thàng công. Ký thất bại, trường này rỗng.
    - error: mô tả lỗi trong trường hợp ký thất bại. Ký số thành công, trường này rỗng.
- signOffice: function (data, funcCallback)
  - Chức năng: ký dữ liệu office (hỗ trợ phiên bản office 2007 trở lên)
  - Tham số
    - data: dữ liệu cần ký. Dữ liệu cần ký được mã hóa base64

- funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.

- Kết quả: kết quả trả về là chuỗi json với định dạng như sau

"\"code\":{0}, \"data\":\"{1}\", \"error\":\"{2}\""

Trong đó các trường có ý nghĩa như sau:

- code: mã trả về. Giá trị và ý nghĩa tương ứng như sau:
  - 0: ký thành công
  - 1: dữ liệu đầu vào rỗng hoặc không đúng định dạng
  - 2: không tìm thấy chứng thư số
  - 3: ký thất bại
  - 4: không tìm thấy private key
  - 5: nguyên nhân không xác định
  - 11: người dùng hủy bỏ
- data: dữ liệu đã ký trong trường hợp ký thàng công. Ký thất bại, trường này rỗng.
- error: mô tả lỗi trong trường hợp ký thất bại. Ký số thành công, trường này rỗng.

➢ signPdf: function (data, funcCallback)

- Chức năng: ký dữ liệu pdf
- Tham số
  - data: dữ liệu cần ký. Dữ liệu cần ký được mã hóa base64
  - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
  - pdfSigner: tham số cấu hình chữ ký pdf. Xem thêm mục 4.2.2.3.
- Kết quả: kết quả trả về là chuỗi json với định dạng như sau

"\"code\":{0}, \"data\":\"{1}\", \"error\":\"{2}\""

Trong đó các trường có ý nghĩa như sau:

- code: mã trả về. Giá trị và ý nghĩa tương ứng như sau:
  - 0: ký thành công
  - 1: dữ liệu đầu vào rỗng hoặc không đúng định dạng
  - 2: không tìm thấy chứng thư số
  - 3: ký thất bại
  - 4: không tìm thấy private key
  - 5: nguyên nhân không xác định
  - 6: tham số số trang chưa được truyền
  - 7: trang đặt chữ ký không hợp lệ
  - 11: người dùng hủy bỏ
- data: dữ liệu đã ký trong trường hợp ký thàng công. Ký thất bại, trường này rỗng.
- error: mô tả lỗi trong trường hợp ký thất bại. Ký số thành công, trường này rỗng.

➢ SignPDFMultiplePages: function (data, funcCallback)

- Chức năng: ký dữ liệu pdf. Đặt chữ ký trên nhiều trang
- Tham số
  - data: dữ liệu cần ký. Dữ liệu cần ký được mã hóa base64
  - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.

- pdfSigner: tham số cấu hình chữ ký pdf. Xem thêm mục 4.2.2.3.

- Kết quả: kết quả trả về là chuỗi json với định dạng như sau

"\"code\":{0}, \"data\":\"{1}\", \"error\":\"{2}\""

Trong đó các trường có ý nghĩa như sau:

- code: mã trả về. Giá trị và ý nghĩa tương ứng như sau:
  - 0: ký thành công
  - 1: dữ liệu đầu vào rỗng hoặc không đúng định dạng
  - 2: không tìm thấy chứng thư số
  - 3: ký thất bại
  - 4: không tìm thấy private key
  - 5: nguyên nhân không xác định
  - 6: tham số số trang chưa được truyền
  - 7: trang đặt chữ ký không hợp lệ
  - 11: người dùng hủy bỏ
- data: dữ liệu đã ký trong trường hợp ký thàng công. Ký thất bại, trường này rỗng.
- error: mô tả lỗi trong trường hợp ký thất bại. Ký số thành công, trường này rỗng.

➢ signCms: function (data, funcCallback)

- Chức năng: ký chuỗi
- Tham số
  - data: dữ liệu cần ký. Dữ liệu cần ký được mã hóa base64
  - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
- Kết quả: kết quả trả về là chuỗi json với định dạng như sau

"\"code\":{0}, \"data\":\"{1}\", \"error\":\"{2}\""

Trong đó các trường có ý nghĩa như sau:

- code: mã trả về. Giá trị và ý nghĩa tương ứng như sau:
  - 0: ký thành công
  - 1: dữ liệu đầu vào rỗng hoặc không đúng định dạng
  - 2: không tìm thấy chứng thư số
  - 3: ký thất bại
  - 4: không tìm thấy private key
  - 5: nguyên nhân không xác định
  - 11: người dùng hủy bỏ
- data: dữ liệu đã ký trong trường hợp ký thàng công. Ký thất bại, trường này rỗng.
- error: mô tả lỗi trong trường hợp ký thất bại. Ký số thành công, trường này rỗng

➢ signHash: function (data, funcCallback)

- Chức năng: ký chuỗi băm
- Tham số
  - data: chuỗi băm
  - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
- Kết quả: kết quả trả về là chuỗi json với định dạng như sau

"\"code\":{0}, \"data\":\"{1}\", \"error\":\"{2}\""

Trong đó các trường có ý nghĩa như sau:

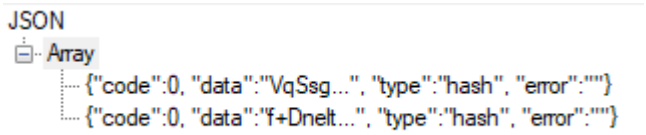
- code: mã trả về. Giá trị và ý nghĩa tương ứng như sau:
  - 0: ký thành công
  - 1: dữ liệu đầu vào rỗng hoặc không đúng định dạng
  - 2: không tìm thấy chứng thư số
  - 3: ký thất bại
  - 4: không tìm thấy private key
  - 5: nguyên nhân không xác định
  - 11: người dùng hủy bỏ
- data: dữ liệu đã ký trong trường hợp ký thàng công. Ký thất bại, trường này rỗng.
- error: mô tả lỗi trong trường hợp ký thất bại. Ký số thành công, trường này rỗng

➢ signArrDataAdvanced: function (arrData, serial, clearPINCache, funcCallback)

- Chức năng: ký dữ liệu theo lô. Trong lô dữ liệu có thể chứa nhiều loại dữ liệu khác nhau.
- Tham số
  - arrData: mảng dữ liệu
  - serial: số serial của chứng thư số sử dụng để ký. Nếu không truyền, plugin sẽ hiển thị popup cho phép người dùng chọn chứng thư.
  - clearPINCache: sử dụng PIN cache hay không?
  - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
- Kết quả: kết quả trả về là mảng chuỗi json với định dạng như sau

["{\"code\":0, \"data\":\"", \"type\":\"hash\", \"error\":\"\"}","{\"code\":0, \"data\":\"", \"type\":\"hash\", \"error\":\"\"}"]

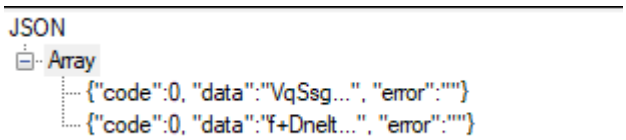
Hình ảnh object json




Trong đó các trường có ý nghĩa như sau:

- code: mã trả về. Giá trị và ý nghĩa tương ứng như sau:
  - 0: ký thành công
  - 1: dữ liệu đầu vào rỗng hoặc không đúng định dạng
  - 2: không tìm thấy chứng thư số
  - 3: ký thất bại
  - 4: không tìm thấy private key
  - 5: nguyên nhân không xác định
  - 6: tham số số trang chưa được truyền
  - 7: trang đặt chữ ký không hợp lệ
  - 8: không tìm thấy thẻ ký số
  - 9: không tham chiếu được tới id thẻ ký số
  - 10: dữ liệu đầu vào chứa một hoặc nhiều chữ ký không hợp lệ

        - 11: người dùng hủy bỏ
    - data: dữ liệu đã ký trong trường hợp ký thàng công. Ký thất bại, trường này rỗng.
    - type: kiểu dữ liệu ký. Hỗ trợ: pdf, docx, xlsx, txt, hash.
    - error: mô tả lỗi trong trường hợp ký thất bại. Ký số thành công, trường này rỗng
- signArrData: function (arrData, type, sigOption, serial, clearPINCache, funcCallback)
  - Chức năng: ký dữ liệu theo lô.
  - Tham số
    - arrData: mảng dữ liệu. Hỗ trợ dữ liệu pdf, xml, office, txt, hash.
    - type: kiểu dữ liệu
    - sigOption: tham số cấu hình chữ ký. Hỗ trợ dữ liệu pdf và xml.
    - serial: số serial của chứng thư số sử dụng để ký. Nếu không truyền, plugin sẽ hiển thị popup cho phép người dùng chọn chứng thư.
    - clearPINCache: sử dụng PIN cache hay không?
    - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
  - Kết quả: kết quả trả về là mảng chuỗi json với định dạng như sau
    ["{\"code\":0, \"data\":\"", \"error\":\"\"}","{\"code\":0, \"data\":\"",  \"error\":\"\"}"]
    Hình ảnh object json




    Trong đó các trường có ý nghĩa như sau:

    - code: mã trả về. Giá trị và ý nghĩa tương ứng như sau:
      - 0: ký thành công
      - 1: dữ liệu đầu vào rỗng hoặc không đúng định dạng
      - 2: không tìm thấy chứng thư số
      - 3: ký thất bại
      - 4: không tìm thấy private key
      - 5: nguyên nhân không xác định
      - 6: tham số số trang chưa được truyền
      - 7: trang đặt chữ ký không hợp lệ
      - 8: không tìm thấy thẻ ký số
      - 9: không tham chiếu được tới id thẻ ký số
      - 10: dữ liệu đầu vào chứa một hoặc nhiều chữ ký không hợp lệ
      - 11: người dùng hủy bỏ
    - data: dữ liệu đã ký trong trường hợp ký thàng công. Ký thất bại, trường này rỗng.
    - error: mô tả lỗi trong trường hợp ký thất bại. Ký số thành công, trường này rỗng.
- getCertInfo: function (funcCallback)
  - Chức năng: lấy thông tin chữ ký số có trên máy client
  - Tham số:
    - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
  - Kết quả: chuỗi json chứa các trường thông tin của chứng thư

- chooseFile: function (funcCallback)
  - Chức năng: cho phép chọn file và trả lại base64 của file
  - Tham số:
    - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong
  - Kết quả: chuỗi base64 của file đã chọn
- setLicenseKey: function (funcCallback)
  - Chức năng: cài đặt license cho plugin. Chỉ những website được cấp license mới có thể sử dụng được plugin
  - Tham số:
    - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
  - Kết quả: kết quả trả về là chuỗi json với định dạng như sau

    "\"code\":{0}, \"data\":\"{1}\", \"error\":\"{2}\""

    Trong đó các trường có ý nghĩa như sau:

    - code: mã trả về. Giá trị và ý nghĩa tương ứng như sau:
      - 1: cài đặt license thành công
      - -1: cài đặt license thất bại
    - data: trường này rỗng
    - error: mô tả lỗi trong trường hợp cài đặt license thất bại
- ValidateCertificate: function (serialNumber, timeCheck, ocspUrl, funcCallback)
  - Chức năng: cho phép kiểm tra hiệu lực của chứng thư số. Plugin sẽ tìm chứng thư số trên máy khách hàng tương ứng với serial để kiểm tra.
  - Tham số:
    - serialNumber: số serial của chứng thư
    - timeCheck: thời gian kiểm tra hiệu lực của chứng thư
    - ocspUrl: link server ocsp
    - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
  - Kết quả:
    - 0: chứng thư số hợp lệ
    - 1: lỗi không xác định
    - 2: chứng thư số hết hạn
    - 3 chứng thư số chưa đến hạn
    - 4: chứng thư số đã bị thu hồi
    - 5: chứng thư số không có quyền ký dữ liệu
    - 6: kiểm tra trạng thái thu hồi của chứng thư không thành công
    - 7: chứng thư số không được cấp bởi CA tin tưởng
    - 8: không lấy được thông tin chứng thư số
    - 9: không lấy được thông tin chứng thư số CA
    - 10: không tìm thấy đường dẫn tới server ocsp
- ValidateCertificateBase64: function (certBase64, timeCheck, ocspUrl, funcCallback)
  - Chức năng: cho phép kiểm tra hiệu lực của chứng thư số.
  - Tham số:

- certBase64: chuỗi mã hóa base64 của chứng thư số
- timeCheck: thời gian kiểm tra hiệu lực của chứng thư
- ocspUrl: link server ocsp
- funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.

- Kết quả:
  - 0: chứng thư số hợp lệ
  - 1: lỗi không xác định
  - 2: chứng thư số hết hạn
  - 3 chứng thư số chưa đến hạn
  - 4: chứng thư số đã bị thu hồi
  - 5: chứng thư số không có quyền ký dữ liệu
  - 6: kiểm tra trạng thái thu hồi của chứng thư không thành công
  - 7: chứng thư số không được cấp bởi CA tin tưởng
  - 8: không lấy được thông tin chứng thư số
  - 9: không lấy được thông tin chứng thư số CA
  - 10: không tìm thấy đường dẫn tới server ocsp

➢ CheckValidTime: function (serialNumber, timeCheck, funcCallback)
- Chức năng: cho phép kiểm tra thời gian hiệu lực của chứng thư số. Plugin sẽ tìm chứng thư số trên máy khách hàng tương ứng với serial để kiểm tra.
- Tham số:
  - serialNumber: số serial của chứng thư
  - timeCheck: thời gian kiểm tra hiệu lực của chứng thư
  - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
- Kết quả:
  - 0: chứng thư số hợp lệ
  - 1: lỗi không xác định
  - 2: chứng thư số hết hạn
  - 3 chứng thư số chưa đến hạn
  - 4: chứng thư số đã bị thu hồi
  - 8: không lấy được thông tin chứng thư số

➢ CheckValidTime: function (certBase64, timeCheck, funcCallback)
- Chức năng: cho phép kiểm tra thời gian hiệu lực của chứng thư số.
- Tham số:
  - certBase64: chuỗi mã hóa base64 của chứng thư số
  - timeCheck: thời gian kiểm tra hiệu lực của chứng thư
  - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
- Kết quả:
  - 0: chứng thư số hợp lệ
  - 1: lỗi không xác định
  - 2: chứng thư số hết hạn
  - 3 chứng thư số chưa đến hạn
  - 4: chứng thư số đã bị thu hồi

- 8: không lấy được thông tin chứng thư số

➢ CheckOCSP: function (serialNumber, timeCheck, funcCallback)

- Chức năng: cho phép kiểm tra thời gian trạng thái thu hồi của chứng thư qua giao thức OCSP. Plugin sẽ tìm chứng thư số trên máy khách hàng tương ứng với serial để kiểm tra.
- Tham số:
  - serialNumber: số serial của chứng thư
  - timeCheck: thời gian kiểm tra hiệu lực của chứng thư
  - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
- Kết quả:
  - 0: chứng thư số hợp lệ
  - 1: lỗi không xác định
  - 4: chứng thư số đã bị thu hồi
  - 5: chứng thư số không có quyền ký dữ liệu
  - 6: kiểm tra trạng thái thu hồi của chứng thư không thành công
  - 7: chứng thư số không được cấp bởi CA tin tưởng
  - 8: không lấy được thông tin chứng thư số
  - 9: không lấy được thông tin chứng thư số CA
  - 10: không tìm thấy đường dẫn tới server ocsp

➢ CheckOCSP: function (certBase64, timeCheck, funcCallback)

- Chức năng: cho phép kiểm tra thời gian trạng thái thu hồi của chứng thư qua giao thức OCSP.
- Tham số:
  - certBase64: chuỗi mã hóa base64 của chứng thư số
  - timeCheck: thời gian kiểm tra hiệu lực của chứng thư
  - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
- Kết quả:
  - 0: chứng thư số hợp lệ
  - 1: lỗi không xác định
  - 4: chứng thư số đã bị thu hồi
  - 5: chứng thư số không có quyền ký dữ liệu
  - 6: kiểm tra trạng thái thu hồi của chứng thư không thành công
  - 7: chứng thư số không được cấp bởi CA tin tưởng
  - 8: không lấy được thông tin chứng thư số
  - 9: không lấy được thông tin chứng thư số CA
  - 10: không tìm thấy đường dẫn tới server ocsp

➢ checkPlugin: function (funcCallback)

- Chức năng: cho phép kiểm tra tính sẵn sàng của plugin
- Tham số:
  - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
- Kết quả:

- 1: thành công
- Khác 1: thất bại

➢ checkPluginAdvanced: function (funcCallback)
- Chức năng: cho phép kiểm tra tính sẵn sàng của plugin, xác thực plugin có đúng là VNPT-CA Plugin hay không?
- Tham số:
  - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
- Kết quả:
  - 1: thành công
  - Khác 1: thất bại

➢ getVersion: function (funcCallback)
- Chức năng: cho phép kiểm tra phiên bản của plugin đang chạy trên máy khách hàng.
- Tham số:
  - funcCallback: hàm javascript callback. Plugin sẽ tự động gọi lại hàm này sau khi nó thực hiện xong.
- Kết quả: phiên bản của plugin.

#### 5.2.2.2. XmlSigner

**a. Mô tả**

XmlSigner là đối tượng javascript chứa các thông số cấu hình chữ ký xml.

**b. Thuộc tính**

Danh sách thuộc tính của đối tượng XmlSigner:

➢ TagSigning: tên của thẻ ký số
➢ NodeToSign: id của thẻ ký số. Nếu thẻ ký số chưa có id thì tham số này sẽ được sử dụng.
➢ TagSaveResult: thẻ lưu chữ ký
➢ NameXPathFilter: tên của thẻ filter theo chuẩn ký xml Xpath Filter. Chưa hỗ trợ.
➢ NameIDTimeSignature: id của thẻ lưu thời gian ký. Chưa hỗ trợ.
➢ DsSignature: tham số cấu hình tiền tố ds của chữ ký. Chưa hỗ trợ.
➢ SigningType: kiểu ký xml (Enveloped, Enveloping, Detach). Plugin hiện tại chỉ hỗ trợ chuẩn ký xml Enveloped.
➢ SigningTime: thời gian ký. Định dạng thời gian: HH:mm:ss dd/MM/yyyy.
➢ CertificateSerial: số serial của chứng thư số sử dụng để ký dữ liệu
➢ ValidateBefore: thuộc tính cấu hình việc xác thực dữ liệu trước khi ký

#### 5.2.2.3. PdfSigner

**c. Mô tả**

PdfSigner là đối tượng javascript chứa các thông số cấu hình chữ ký pdf.

**d. Thuộc tính**

Danh sách thuộc tính của đối tượng PdfSigner:

➢ page: trang đặt chữ ký
➢ llx: hoành độ góc dưới bên trái của hình chữ nhật chứa chữ ký.

- lly: tung độ góc dưới bên trái của hình chữ nhật chứa chữ ký.
- urx: hoành độ góc trên bên phải của hình chữ nhật chứa chữ ký.
- ury: tung độ góc trên bên phải của hình chữ nhật chứa chữ ký
- SigTextSize: cỡ chữ trong chữ ký
- Signer: người ký
- Description: mô tả
- OnlyDescription: chỉ hiển thị mô tả?
- SigningTime: thời gian ký. Định dạng thời gian: HH:mm:ss dd/MM/yyyy.
- CertificateSerial: số serial của chứng thư số sử dụng để ký dữ liệu
- SigColorRGB: màu chữ, mã rgb.
- ImageBase64: chuỗi base64 của ảnh hiển thị trên chữ ký
- SetImageBackground: cài đặt ảnh làm nền chữ ký?
- PagesArray: mảng chứa danh sách trang đặt chữ ký

### 5.3. Ví dụ tích hợp

Ví dụ tích hợp hàm ký dữ liệu xml:

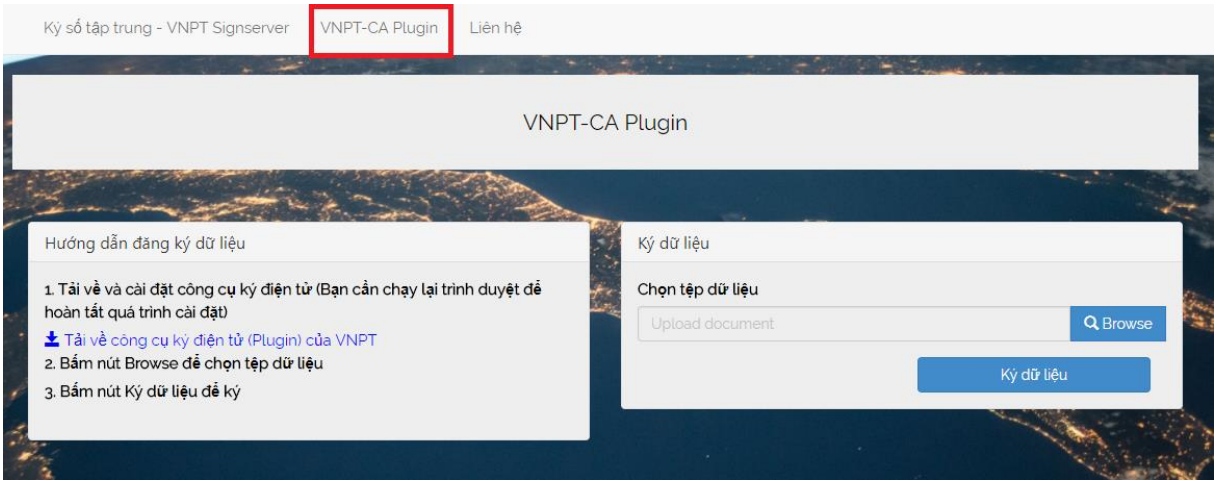
```
// dataJson: chuỗi json kết quả.
// Plugin sẽ tự động gọi lại hàm signCallback sau khi ký xong
// và đẩy kết quả ký vào dataJson
function signCallback(dataJson) {
    var jsObj = JSON.parse(dataJson);
    if (jsObj.code != 0) {
        alert("Ký thất bại. Mã lỗi: " + jsObj.error);
        return;
    }
    else
    {
        alert("Ký thành công. Dữ liệu đã ký: " + jsObj.data);
    }
}

function sign() {
    var data = ""; // base64 của dữ liệu cần ký
    // signCallback: plugin tự động gọi làm hàm này sau khi ký xong
    vnpt_plugin.signXML(data, signCallback);
}
```

## 6. THỬ NGHIỆM

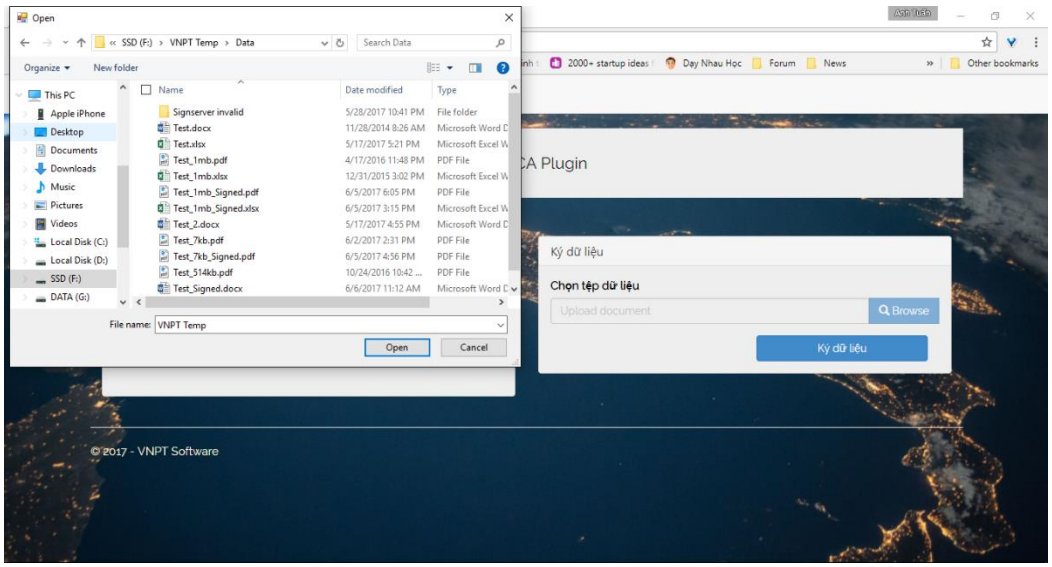
Quý khách hàng mở trình duyệt và truy cập: http://kyso.vnpt-ca.vn/Module/DemoSigning

Trên menu chọn VNPT CA Plugin hệ thống hiện thị giao diện như hình dưới:

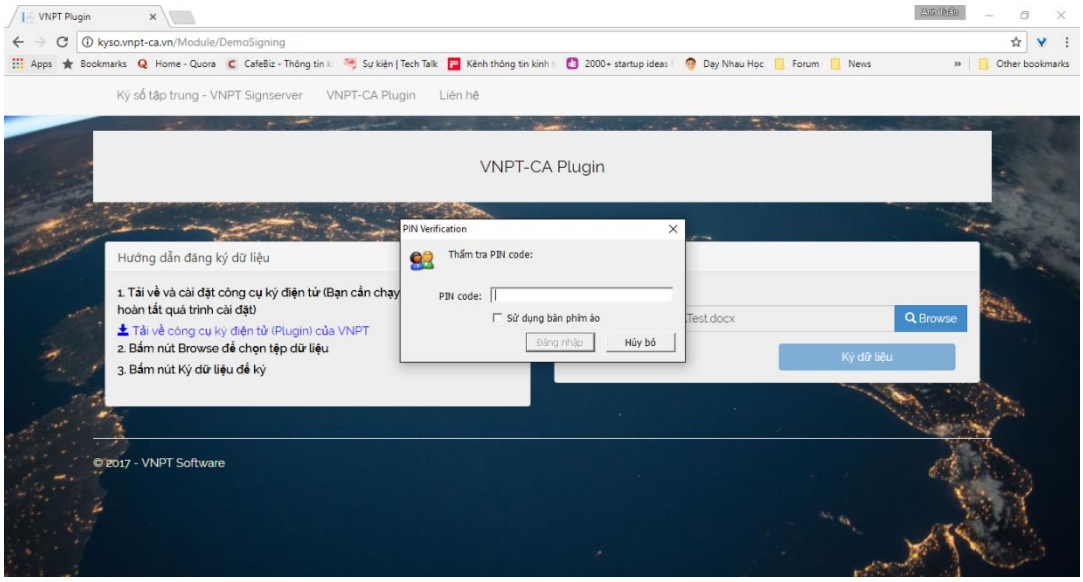



Quý khách hàng vui long thực hiện theo 3 bước như hình trên

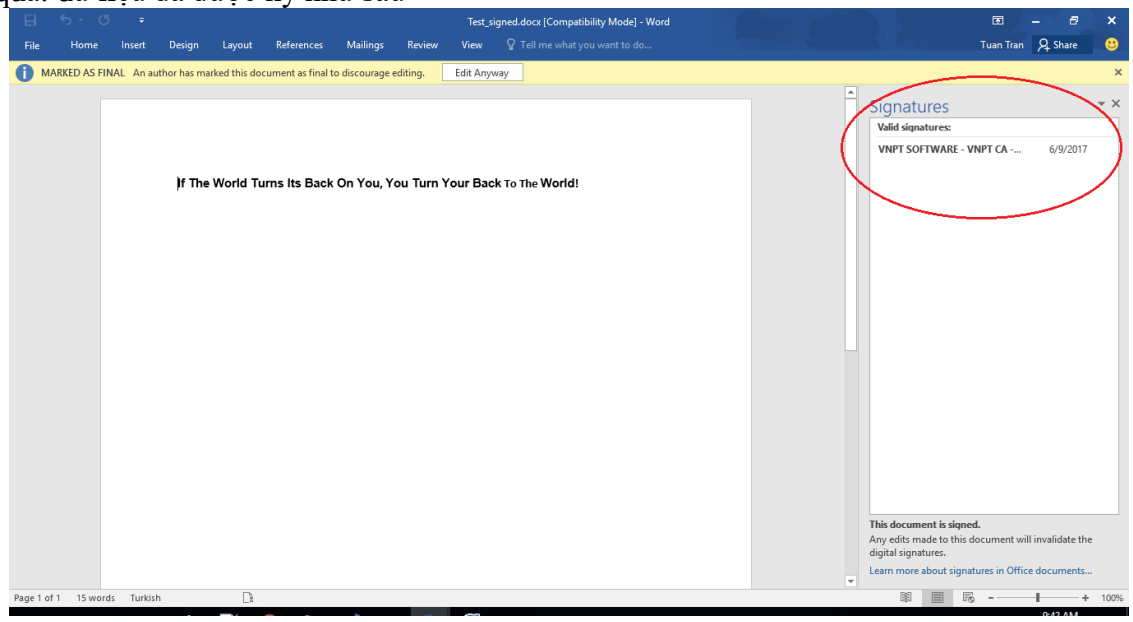
Tích hợp hàm chọn file. Plugin hiển thị giao diện chọn file như sau



Tích hợp hàm ký dữ liệu. Plugin tương tác với token, yêu cầu khách hàng nhập mã PIN để ký số




Kết quả: dữ liệu đã được ký như sau




*Thông tin hỗ trợ:*

*Liên hệ: Nguyễn Đăng Huy sđt: 0886241199 email: nguyendanghuy@vnpt.vn*