# Hướng dẫn test chrome\_Extension\_ver1

# (Tiện ích mở rộng cho trình duyệt web chrome)

## Giới thiệu về sản phẩm

1. Giới thiệu

Chrome Extension là một tiện ích mở rộng được cài trên trình duyệt web chrome cho phép ký số các tài liệu trên đó. Việc ký số sẽ cho phép ký trên các tài liệu được đưa lên (các file .doc, .pdf, .txt…) và trả về tài liệu kèm theo chữ ký trên tài liệu đã được xác thực.

Sản phẩm hiện tại:

* Input: Chuỗi HASH là một bảng băm (chuỗi ký tự không cho phép thay đổi) cần ký.
* Output: chữ ký trên chuỗi hash đầu vào.

1. Ghi chú về sản phẩm:

Chuỗi hash là một bảng băm mà hiện tại đang được fix cứng trong code, trong các ver mở rộng sau này chuỗi hash này sẽ đại diện cho chuỗi băm tài liệu đầu vào.

Sản phẩm bao gồm 1 file setup: cho phép cài đặt ứng dụng trên máy và tự động cài đặt extension trên chrome. Mô hình cài dặt tương tự như khi cài đặt IDM download, sau khi cài đặt chrome sẽ tự dộng tích hợp extension của ứng dụng.

## Các khái niệm cần nắm

1. **Chữ ký số là gì?**

Về căn bản, khái niệm chữ ký số cũng giống như chữ viết tay. Bạn dùng nó để xác nhận lời hứa hay cam kết của mình và sau đó không thể rút lại được. Chữ ký số không đòi hỏi phải sử dụng giấy mực, nó gắn đặc điểm nhận dạng của người ký vào một bản cam kết nào đó.

**Chữ ký số** dựa trên công nghệ mã hóa công khai (RSA): mỗi người dùng phải có 1 cặp khóa (keypair) gồm khóa công khai (public key) và khóa bí mật (private key)

**Private key** là một khóa trong cặp khóa thuộc hệ thống mã không đối xứng được dùng để tạo chữ ký số.

**Public key** là một khóa trong cặp khóa thuộc hệ thống mã không đối xứng, được sử dụng để kiểm tra chữ ký số được tạo bởi khóa bí mật tương ứng trong cặp khóa.

**Ký số** là việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu.

**Người ký** là thuê bao dùng đúng khóa bí mật của mình để ký số vào một thông điệp dữ liệu dưới tên của mình.

**Người nhận** là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng các chứng thư số của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.

1. **Chứng thư số là gì**

Chứng thư số là một dạng chứng thư điện tử do tổ chức cung cấp dịch vụ chứng thực chữ ký số cấp. Chứng thư số có thể được xem như là "chứng minh thư" để sử dụng trong môi trường của máy tính và internet.

Chứng thư số được sử dụng để nhận diện một cá nhân, một máy chủ, hay là một vài đối tượng khác và gắn định danh của đối tượng đó với một public key, được cấp bởi những tổ chức có thẩm quyền xác định nhận danh và cấp chứng thư số.

Chứng thu số được tạo bởi nhà cung cấp dịch vụ chứng thực trong đó chứa public key và các thông tin của người dùng theo chuẩn X.509. Khóa bí mật của chữ ký số bắt buộc phải lưu trữ trong một thiết bị phần cứng chuyên dụng là USB Token hoặc SmartCard được cung cấp bởi nhà cung cấp. Các thiết bị này đảm bảo khóa bí mật không bị copy hay bị virus phá hỏng.

1. Khái niệm token

**Token** là một thiết bị có lưu trữ thông tin chứng thư số của cá nhân hay doanh nghiệp.

**Nội dung của chứng thư số**

•       Tên của thuê bao.

•       Số hiệu của chứng thư số (số seri)

•       Thời hạn có hiệu lực của chứng thư số

•       Tên của tổ chức chứng thực chữ ký số (Ví du: VNPT-CA)

•       Chữ ký số của tổ chức chứng thực chữ ký số.

•       Các thư hạn chế về mục đích, phạm vi sử dụng của chứng  số.

•       Các hạn chế về trách nhiệm của tổ chức cung cấp dịch vụ chứng thực chữ ký số.

•       Các nội dung cần thiết khác theo quy định của Bộ Thông Tin Truyền Thông.



Một hình ảnh về USB token

1. Khái niệm PKCS11, CSP

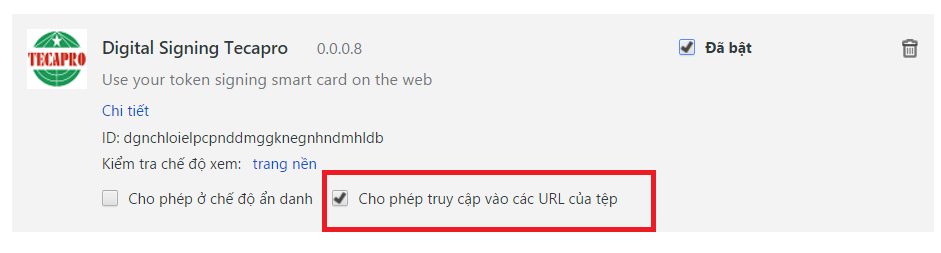
PKCS11 là một chuẩn mã hóa khóa công khai (public key) dùng để truy cập và kết nối đến USB token.

CSP là một thư viện các thuật toán mã hóa (.dll) trên winStore.

## Cách sử dụng sản phẩm và kết quả mong muốn

1. Trình tự cài đặt ứng dụng

* Cài đặt ứng dụng



* Cài đặt manager cho usb token (test ký với usb token).

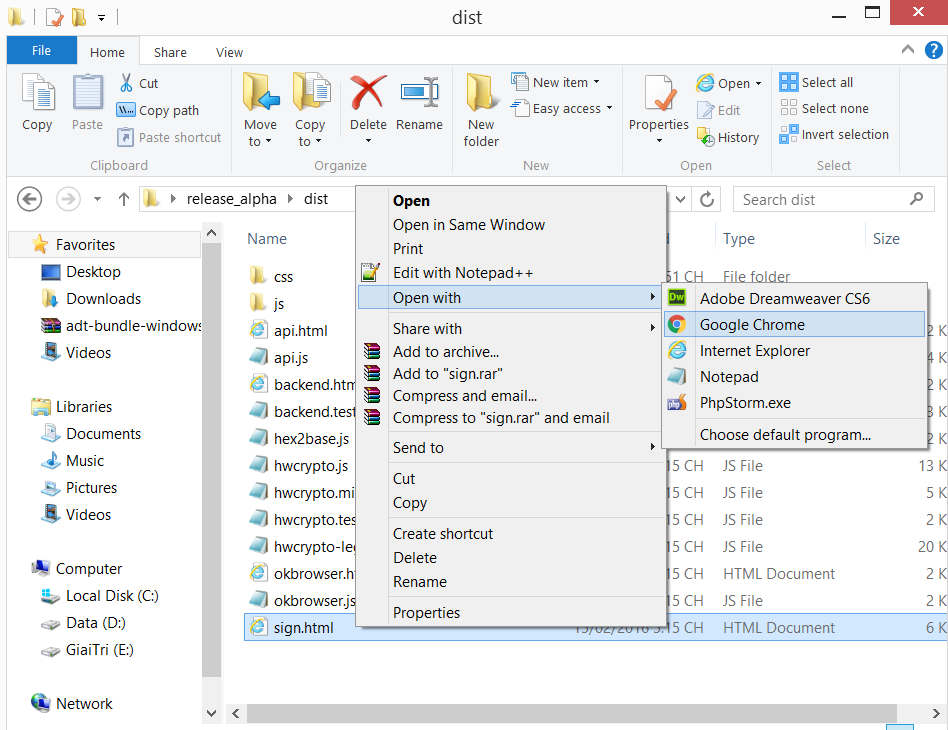
Vào trang chủ của token tải bộ manager và cài đặt

Vd: <http://vnpt-ca.vn/khach-hang/tai-lieu?listVM.id=10>

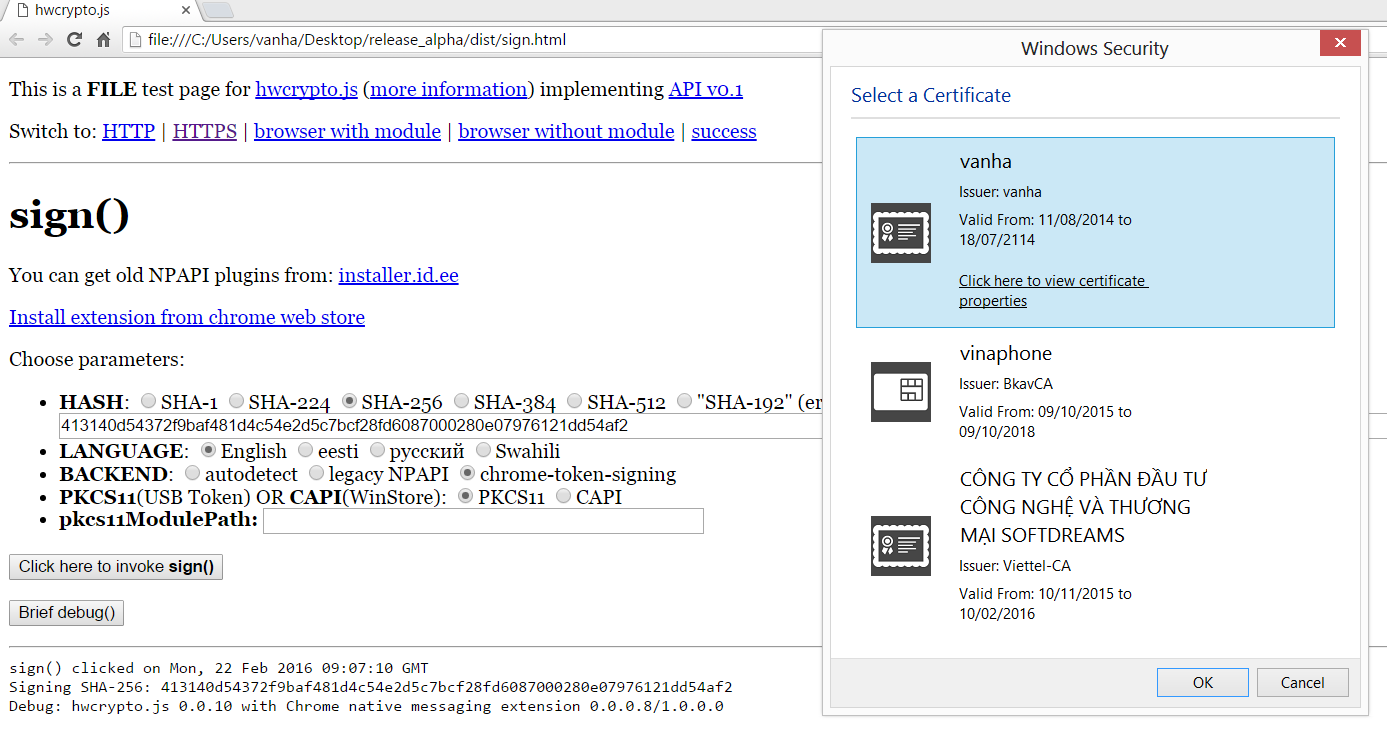
* Cài đặt file p12 (test với CSP)

1. Trình tự tiến hành test

* Vào trang sign.html trong thư mục cài đặt release\_alpha/dist bằng trình duyệt chrome:



* Tiến hành test trang



* Hash: chuỗi ký tự đăị diện cho chuỗi hash khi băm dữ liệu cần ký.
* Language: chọn gì cũng được.
* Backend: chrome-token-signing.
* Chọn PKCS11 khi sử dụng chứng thư từ USB token. Đồng thời bắt buộc điền đúng pkcs11ModulPath phía dưới để tiến hành ký.
* Chọn CAPI khi sử dụng chứng thư được cài từ file P12. Nếu chọn mục này không cần phải điền pkcs11ModulPath (mặc định là NULL).
* Kết quả mong muốn:

Hiển thị được CERT\_id và chữ ký (được biểu diễn bằng chuỗi hex)

