GIẢI PHÁP TÍCH HỢP VNPT-CA SIGNSERVER

Hà Nội, 03– 2017

MỤC LỤC

I. GIỚI THIỆU

1.1. Mục đích

Tài liệu mô tả giải pháp tích hợp VNPT-CA Signserver vào hệ thống ứng dụng của khách hàng, giải quyết các vấn đề ký số.

1.2. Thuật ngữ và từ viết tắt

VNPT-CA	Chứng thư số do VNPT-CA cấp phát
CTDT	Phòng giải pháp chứng thực điện tử
KH	Khách hàng
CTS	Chứng thư số
PKI	Public Key Infrastructure (nền tảng khóa công khai)
OCSP	Online Certificate Status Protocol
CRL	Certificate Revocation List
CA	Certificate Authority – Nhà cung cấp chứng thư số
WORKER	Thuật ngữ mô tả đối tượng chứa thông tin cấu hình các chức năng (chức năng ký số, xác thực,…)
HSM	Hardware Security Module – Thiết bị chuyên dụng sử dụng để lưu chữ chứng thư số, cặp khóa

II. NHU CẦU TÍCH HỢP KÝ SỐ

2.1. Khảo sát hệ thống

Hiện nay, phần lớn các tổ chức, doanh nghiệp đều đang sử dụng văn bản, tài liệu dưới dạng file mềm để phục vụ cho công việc điều hành văn bản trong nội bộ hay giao dịch với đối tác, khách hàng bên ngoài. Bên cạnh đó, việc ký số lên tài liệu cũng đang được nhiều tổ chức, doanh nghiệp xem xét áp dụng để mang lại tính pháp lý cũng như tính xác thực cho tài liệu. Do đó, nhu cầu tích hợp chữ ký số vào hệ thống tin học trong tổ chức, doanh nghiệp là rất lớn.

Giải pháp VNPT -CA Signserver (Signserver) được xây dựng để đáp ứng tất cả các nhu cầu tích hợp ký số của các tổ chức, doanh nghiệp.

Hệ thống ký số VNPT-CA Signserver: là ứng dụng webservice cung cấp các chức năng ký, xác thực dữ liệu. Các chức năng được cung cấp dưới dạng webservice làm cho việc tích hợp trở lên đơn giản. Signserver được thiết kế để dễ dàng nâng cấp và mở rộng các chức năng, được xây dựng phù hợp để triển khai trên các môi trường máy chủ khác nhau như: windows server, centos, ubuntu,…

Hệ thống cung cấp các API ký số, cấu hình dạng webservice, cung cấp các dịch vụ dành cho phân hệ Client và phân hệ Admin như sau:

- Phân hệ Client: thực hiện ký, xác thực dữ liệu (pdf, office, xml, txt …), kiểm tra hiệu lực của chứng thư số.
- Phân hệ Admin: thực hiện cấu hình và cài đặt các chức năng.

2.2. Yêu cầu tích hợp SignServer

Các hệ thống cần tích hợp SignServer:

- Các hệ thống ký số tập trung, thường là các hệ thống quản trị người dùng, người dùng trong hệ thống đó có nhu cầu sử dụng chữ ký số riêng của mình để ký dữ liệu (chữ ký số tương ứng với từng người dùng sẽ được lưu trên Server).
- Sử dụng chữ ký số đại diện cho tổ chức, doanh nghiệp

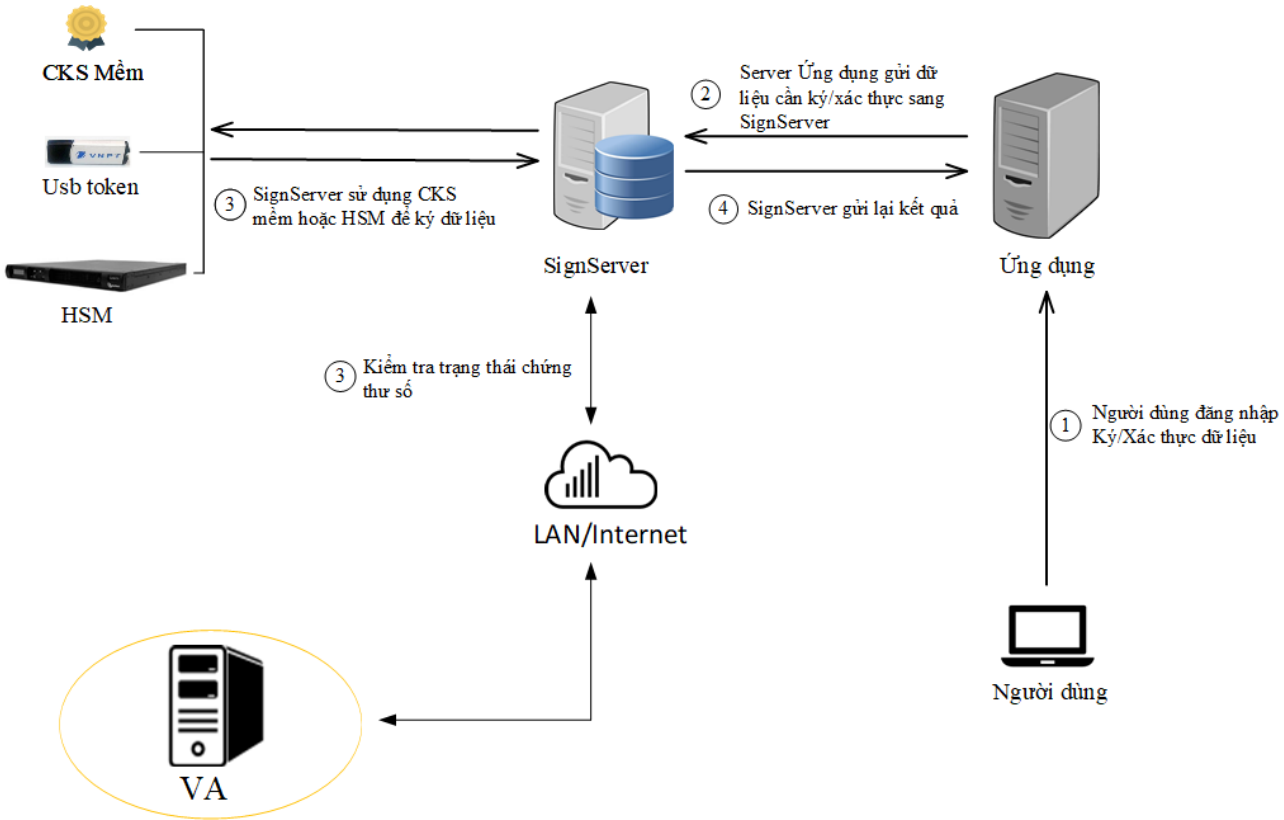
III. MÔ HÌNH HỆ THỐNG

3.1. Mô tả

Hệ thống Signserver có thể dễ dàng tích hợp vào các hệ thống có sẵn của khách hàng.

3.2. Mô hình

Mô hình hệ thống sau khi tích hợp Signserver như sau:



Các thành phần

- **SignServer**: là hệ thống ứng dụng VNPT-CA Signserver
- **VA**: là server kiểm tra hiệu lực chứng thư số (server OCSP,..) của nhà cung cấp dịch vụ chứng thực điện tử (CA)
- **Ứng dụng**: là ứng dụng của khách hàng (Hệ thống Hóa đơn Điện tử, Hệ thống quản lý văn bản,…)

Luồng xử lý

- Bước 1: Người dùng sử dụng ứng dụng và thực hiện ký/xác thực dữ liệu
- Bước 2: Ứng dụng gửi dữ liệu cần ký/xác thực sang Signsever
- Bước 3: Signserver xử lý
    - Ký dữ liệu: Signserver tương tác với HSM hoặc chứng thư số mềm để ký
    - Xác thực dữ liệu: Signserver kiểm tra tính toàn vẹn của dữ liệu đồng thời kết nối với VA để kiểm tra hiệu lực chứng thư số
- Bước 4: SignServer trả lại kết quả cho ứng dụng

Các chức năng Signserver cung cấp

Sigserver cung cấp các chức năng dành cho phần hệ Client và phần hệ Admin như sau:

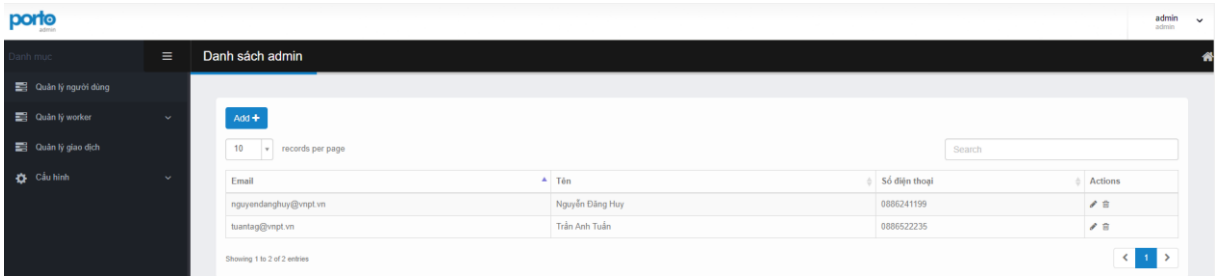
- **Phân hệ Client**
    - Ký dữ liệu
        - Ký dữ liệu office, openoffice, xml, pdf, txt. Signserver tương tác với các thiết bị lưu trữ chứng thư số, cặp khóa chuyên dụng như HSM, Usb token để ký số.
        - Chỉnh sửa, cấu hình vị trí đặt chữ ký, màu, kích thước chữ, ảnh trên chữ ký pdf.
        - Cho phép ký toàn bộ dữ liệu hoặc ký dữ liệu trên một thẻ của dữ liệu xml.
    - Xác thực dữ liệu
        - Cho phép kiểm tra tính toàn vẹn của dữ liệu office, xml, pdf, txt
        - Kiểm tra hiệu lực của chứng thư số tại thời điểm ký.
    - Kiểm tra hiệu lực của chứng thư số
        - Kiểm tra thời gian chứng thư số có hiệu lực
        - Kiểm tra trạng thái thu hồi của chứng thư số thông qua hai giao thức OCSP hoặc CRL.
        - Kiểm tra quyền ký của chứng thư
        - Kiểm tra xem chứng thư số có được cung cấp bởi một CA tin tưởng hay không?
- **Phân hệ Admin**: cho phép quản trị hệ thống qua giao diện web với các chức năng sau:
    - Quản lý quản trị viên hệ thống
    - Quản lý worker

- Quản lý giao dịch
- Cấu hình

Chi tiết các chức năng Phân hệ Admin

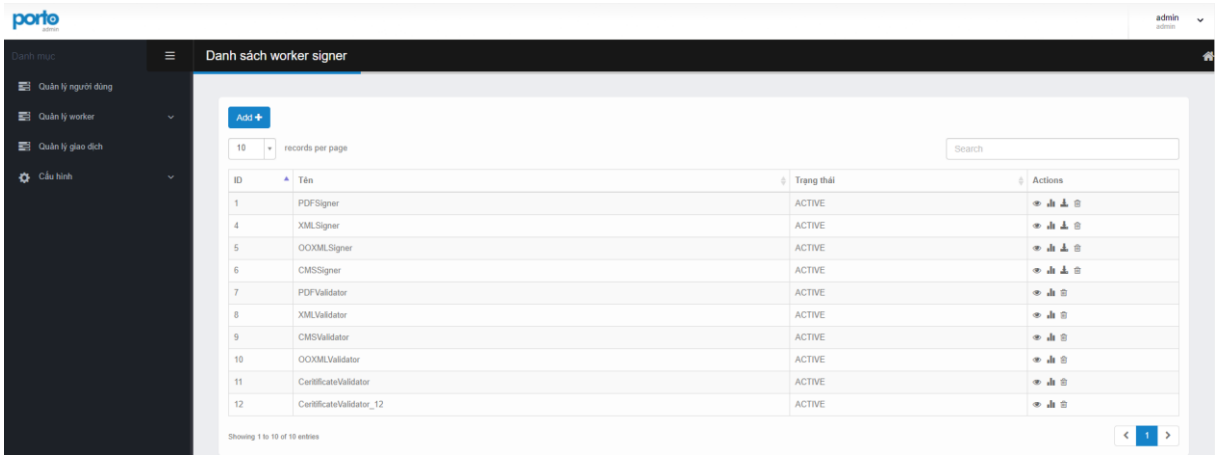
- Quản lý quản trị viên hệ thống

Cho phép thêm, sửa, xóa thông tin quản trị viên, người có thể đăng nhập vào hệ thống.



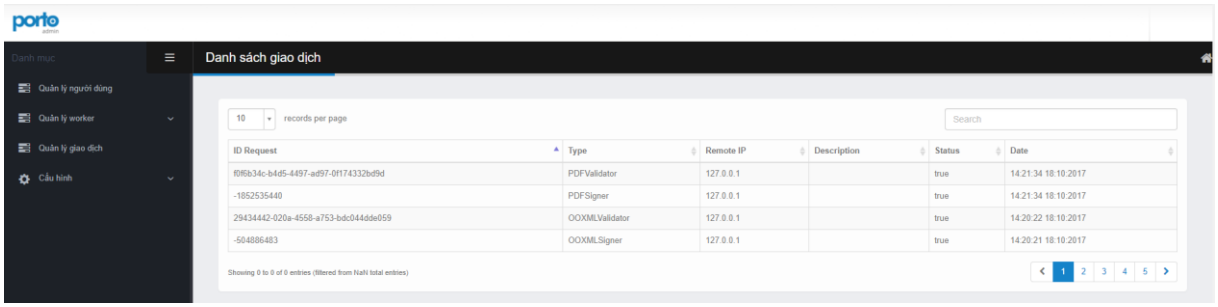
- Quản lý worker

Cho phép quản lý, cấu hình các chức năng ký, xác thực, kiểm tra hiệu lực chứng thư số,…



- Quản lý giao dịch

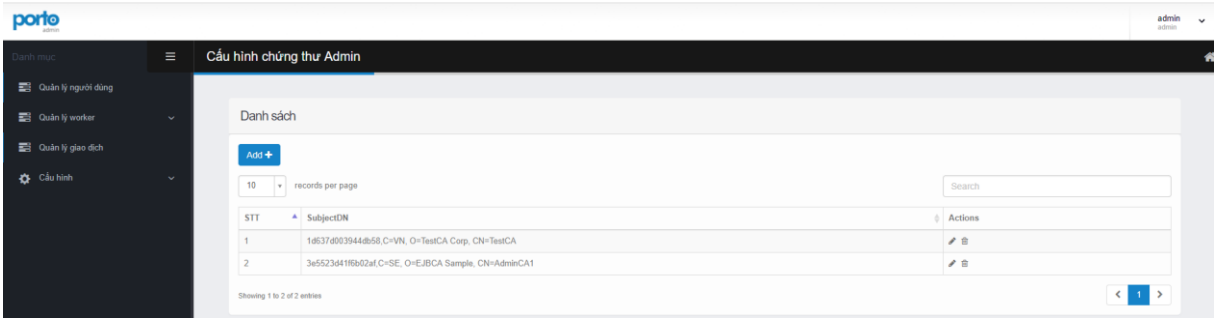
Cho phép xem, tìm kiếm, thống kê các giao dịch ký số đã thực hiện, thông tin về giao dịch như loại file đã ký, trạng thái ký,…



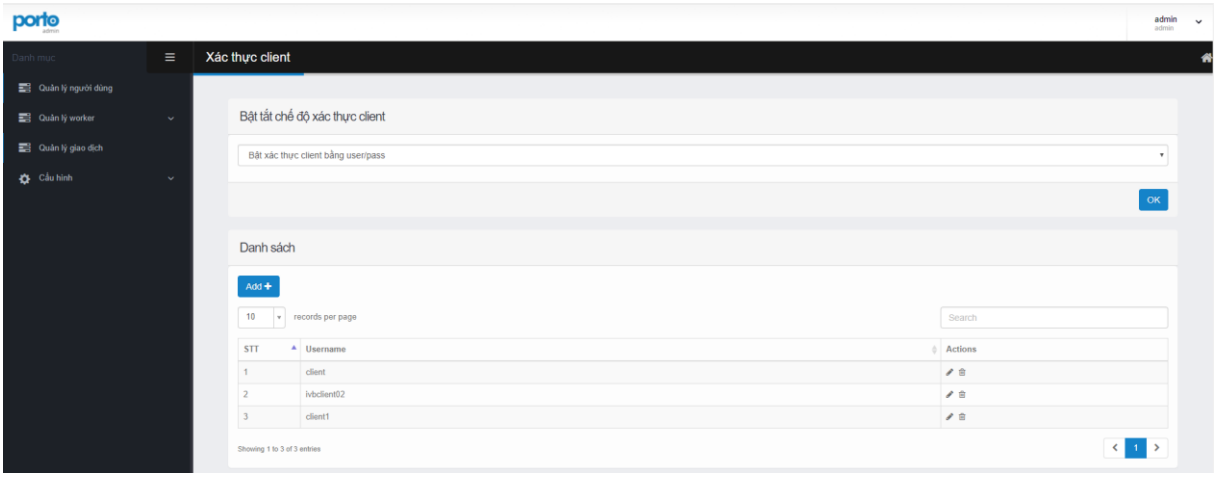
- Cấu hình

Cho phép cấu hình chứng thư số admin, cấu hình bật tắt chế độ xác thực client, thêm, sửa, xóa tài khoản client,…

Giao diện cấu hình chứng thư số admin:



Giao diện cấu hình chế độ xác thực client



3.3. Đánh giá

- Giải pháp tích hợp VNPT-CA Signserver là linh động, bảo mật, phù hợp với tất các hệ thống.
- Hệ thống triển khai tiện lợi, đơn giản hóa quá trình ký số của người dùng.
- Hệ thống ký số tương thích với tất cả chứng thư số của các nhà cung cấp được cấp phép bởi Bộ Thông tin và Truyền thông.

IV. THÔNG SỐ KỸ THUẬT

4.1. Yêu cầu hệ thống

Hệ điều hành

- Windows server phiên bản 2008 trở lên
- Centos phiên bản 6.5 trở lên.

Java: java phiên bản 7 trở lên.

Cơ sở dữ liệu: cơ sở dữ liệu hỗ trợ các phiên bản sau

- MySQL bản 5.5 trở lên
- Oracle Database bản 10 trở lên
- SQL Server bản 2008 trở lên.
- PostgreSQL phiên bản 9 trở lên

Application Server: WildFly 9.0.0.

4.2. Hiệu năng hệ thống

Với server có thông số CPU 8 core, RAM 16G, HDD 1T, hiệu năng như sau:

- Ký/Xác thực: 2000 Tran/s – 1 Tran ~ 10Kb
- Ký/Xác thực : 100 Tran/s – 1 Tran ~ 2Mb

V. THỬ NGHIỆM

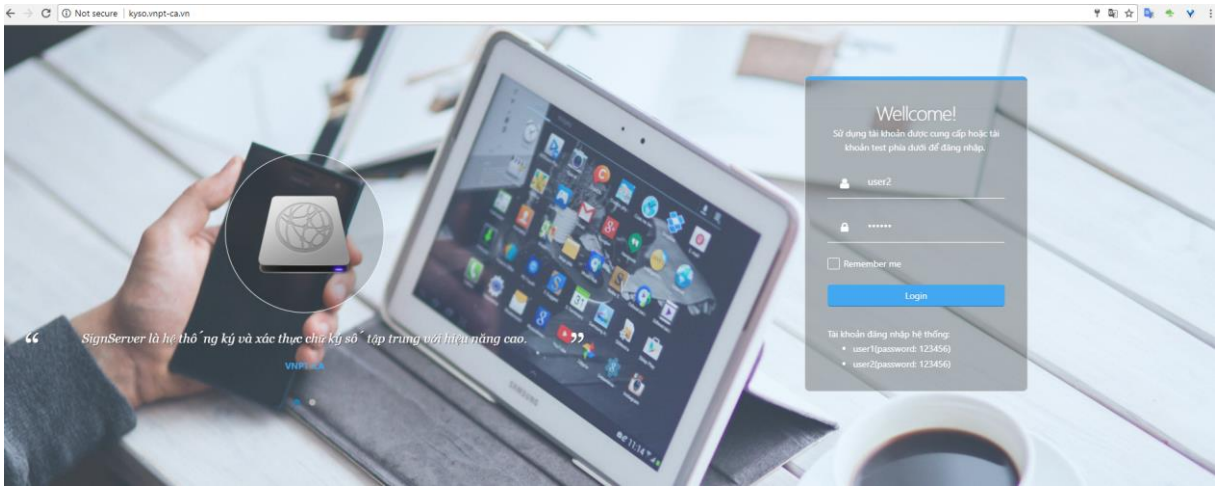
Quý khách hàng mở trình duyệt và truy cập: http://kyso.vnpt-ca.vn/

Đây là website đã được tích hợp với hệ thống ký số VNPT-CA Signserver.

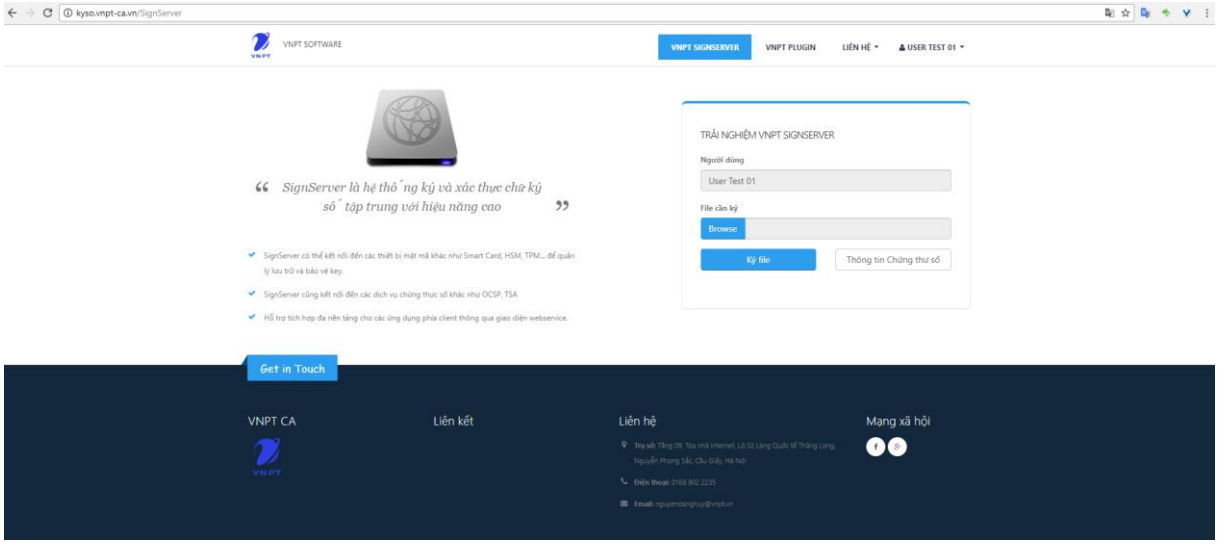
Sử dụng các tài khoản sau để đăng nhập hệ thống:

user1(password: 123456), user2(password: 123456)

Giao diện đăng nhập

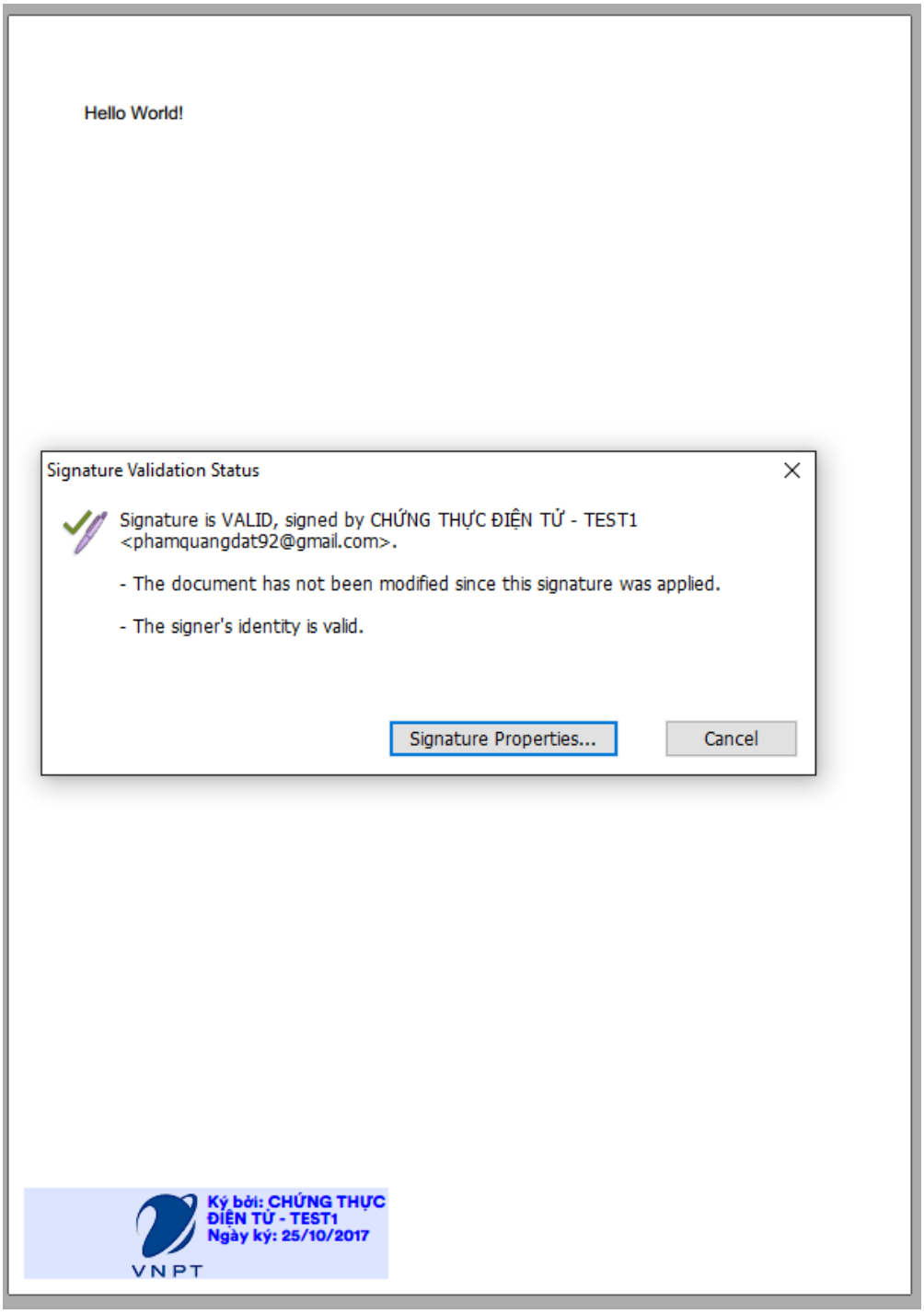


Để thử nghiệm ký số, chọn nút "Browse" tìm file cần ký, sau đó chọn "Ký file" để ký số.



Kết quả: người dùng tải file đã ký.

Hình ảnh file pdf đã được Signserver ký và gửi lại cho Website:



Thông tin liên hệ:

Nguyễn Đăng Huy - 0886241199