**DOCUMENT DESCRIBING VIRTUAL CSP**

Author: Nam

Email: dk.nam855@gmail.com

1. **Introduction to Virtual CSP**

**Current State of Digital Signing with HSM:** Enterprises deploying HSM (Hardware Security Module) typically use it only for signing electronic invoices. Integrating digital signatures with systems such as Tax, Customs, and other software poses significant challenges.

**Virtual CSP (also known as Virtual Cryptographic Service Provider)** enables Windows applications to sign directly to an HSM (server) via an API.

Virtual CSP allows end-users to perform digital signing with applications like Acrobat Reader/Foxit, MS Office, Tax, Customs, etc., directly from their own machines (the signing process is similar to using a USB Token)

1. **Demo Server Setup (Using P12 for Signing; in Practice, HSM Would Be Used)**

**Implementation Guide:**

* Server: Tomcat 8
* Included War Package
* Adjust the path and password of the P12 file in config.json (this file is located in the Conf folder of Tomcat).

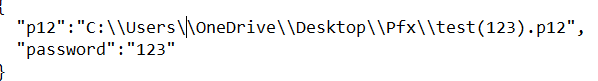
**Two APIs:**

1. getbase64cert: Retrieves the base64 value of the digital certificate.
2. signdata: Signing function.

For the purpose of demonstrating Virtual CSP functionality, the API server is kept simple and serves only to sign at the server (HSM). In real-world use, this API would be provided by the enterprise.

The demo API uses a P12 file for signing. Configure the P12 file as follows:

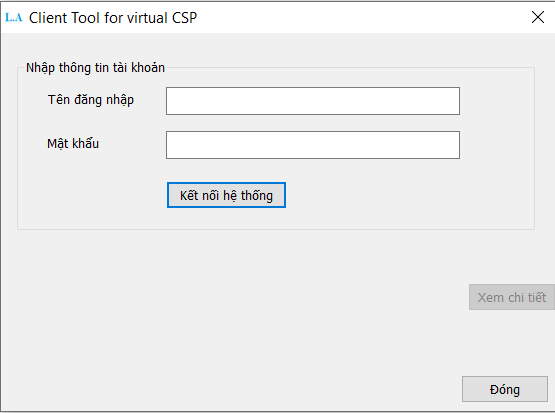
In the conf folder of Tomcat, edit the config.json file to adjust the path and password of the P12 file.



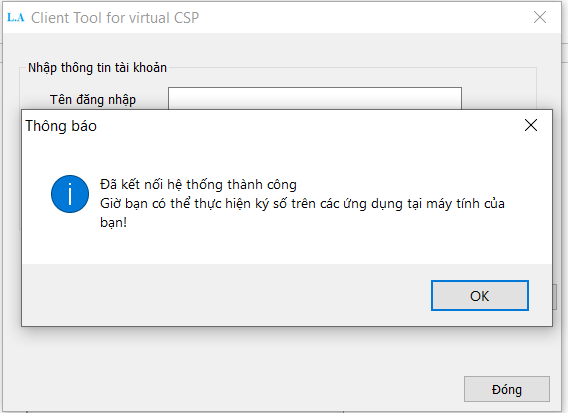
1. **Virtual CSP Installation**

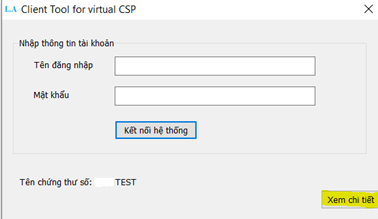
Tested on Windows 7/10/11:

* Install the setup package.
* Run the tool “ClienToolvCSP.exe”.
  + The tool is for demo purposes only, so no “username” or “password” is required.
  + Click the “Connect to System” button to check the digital certificate on the server



Kết quả nhận được thông báo





A notification will be displayed.

You can click “View Details” to show detailed information about the digital certificate. This certificate will be used for signing on the user’s machine.

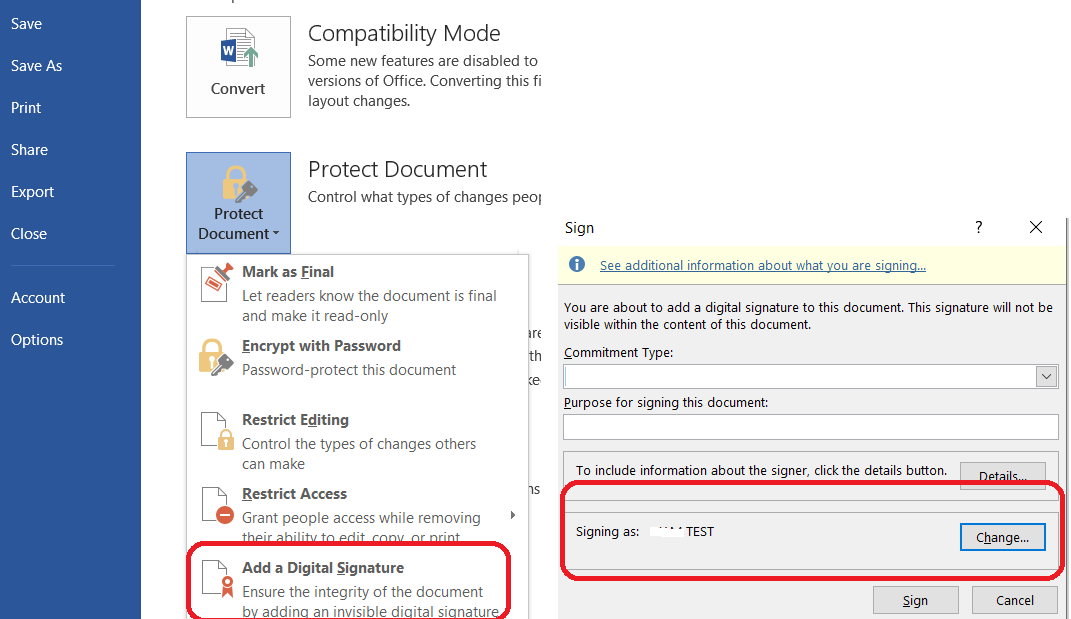
Once completed, the user can sign with Windows applications.

1. **Testing Procedure**

Before testing, ensure the computer has Virtual CSP installed and the “ClienToolvCSP.exe” tool has been run to retrieve the digital certificate information.

Open the application for testing; the signing process will be similar to using a USB Token

Example with Word:



 Open Word and select the digital signing feature.

 The Virtual CSP PIN entry interface will appear (for the demo, any PIN will work ^^). Click “OK” to complete



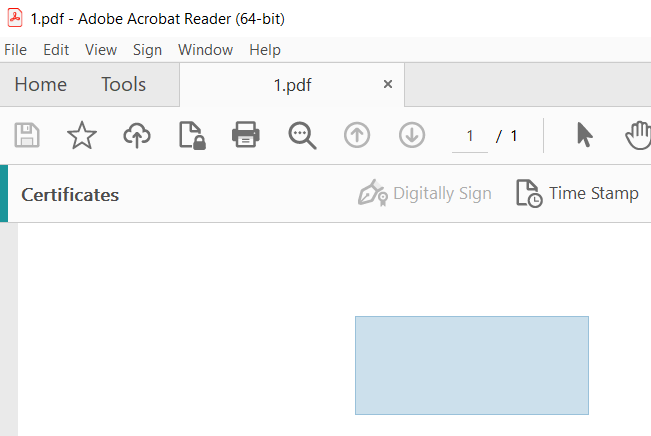
Example with Acrobat

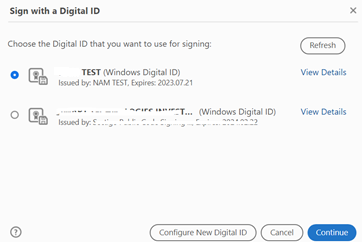
 Select the digital signing feature in Acrobat.

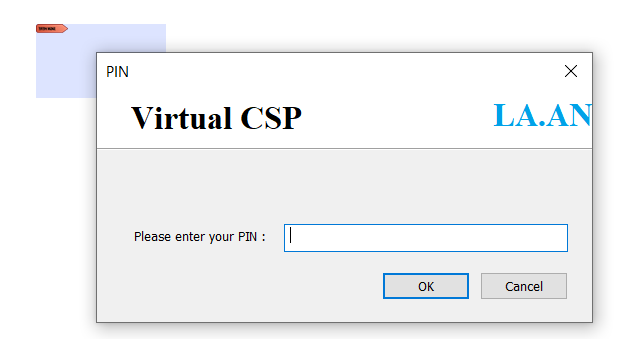
 Choose the user’s digital certificate.

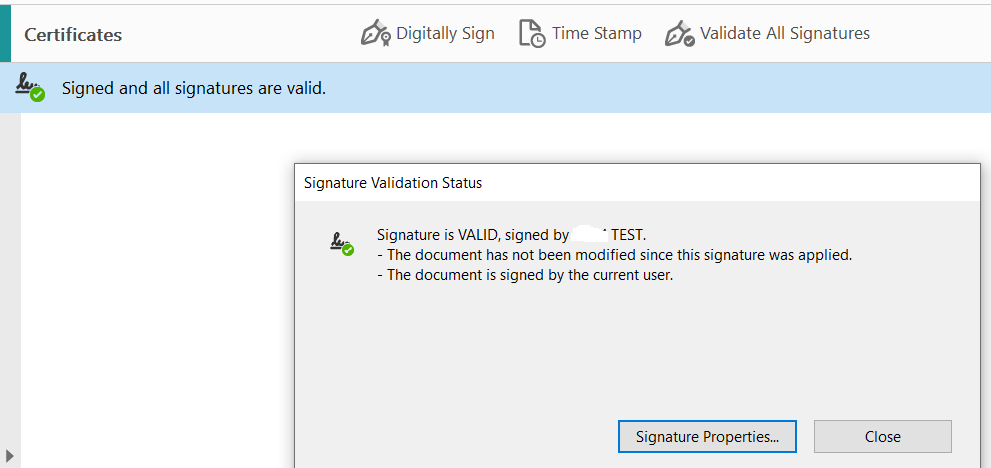
 The Virtual CSP PIN entry interface will appear. Click “OK”.

 Signing is completed; check the signature status.









**Conclusion**

This is a sample test aimed at demonstrating the functionality of Virtual CSP, so the server API is kept simple.

In real-world deployment, Virtual CSP will be customized to suit the APIs provided by the enterprise.