

Захист від зміни бінарного файлу

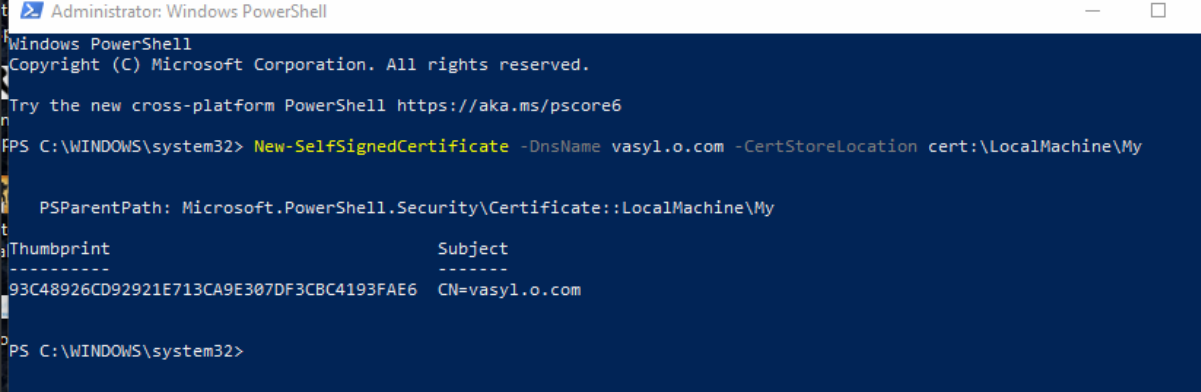
Мета

Навчитися підписувати виконувані файли.

Завдання

- створити сертифікат
- проінсталювати його в систему, щоб він був "довіреним"
- використовуючи проект будь-якої попередньої роботи, виконати підпис виконуваного файлу за допомогою утиліти SignTool (або JarSigner)
- виконати верифікацію підпису (бажано на рівні самого кода при завантаженні додатка):
 - чи є підписаний сертифікат валідним
 - чи не було (бінарної) зміни файлу та його код цілісний

Хід роботи



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> New-SelfSignedCertificate -DnsName vasy1.o.com -CertStoreLocation cert:\LocalMachine\My

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                               Subject
-----
93C48926CD92921E713CA9E307DF3CBC4193FAE6  CN=vasyl.o.com

PS C:\WINDOWS\system32>
```

Рис 1 - Створення сертифікату

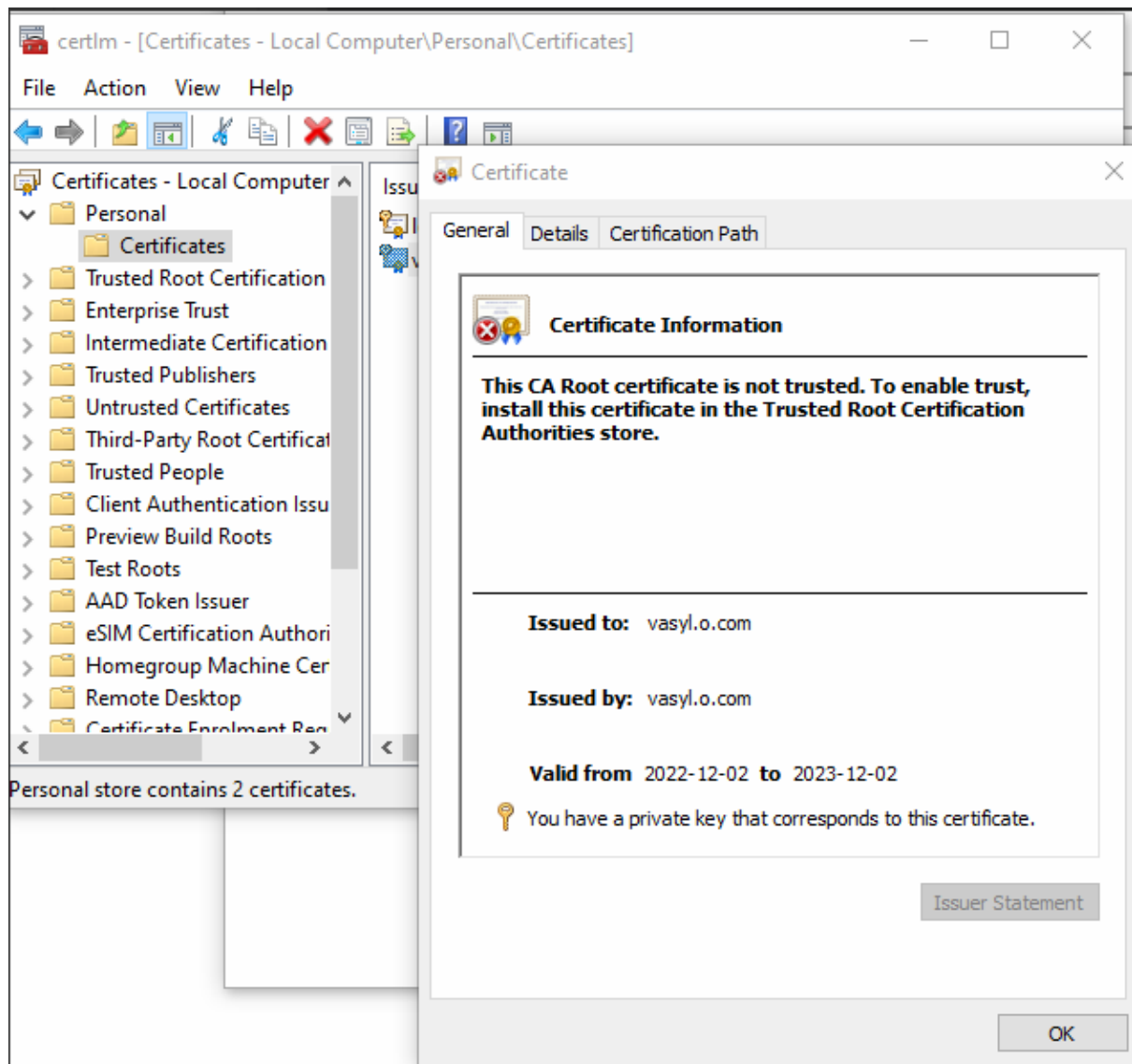


Рис 2 - Не довірений сертифікат

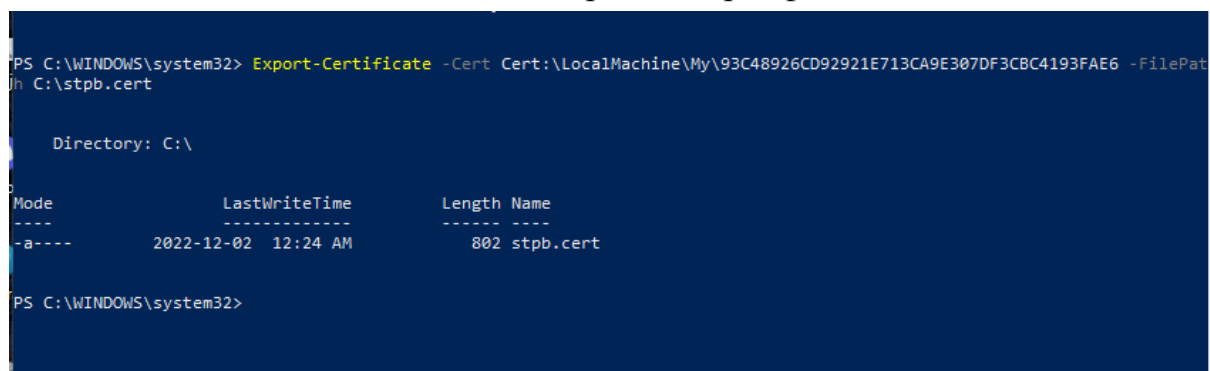


Рис 3 - експорт сертифікату на диск та імпорт в довірені сертифікати

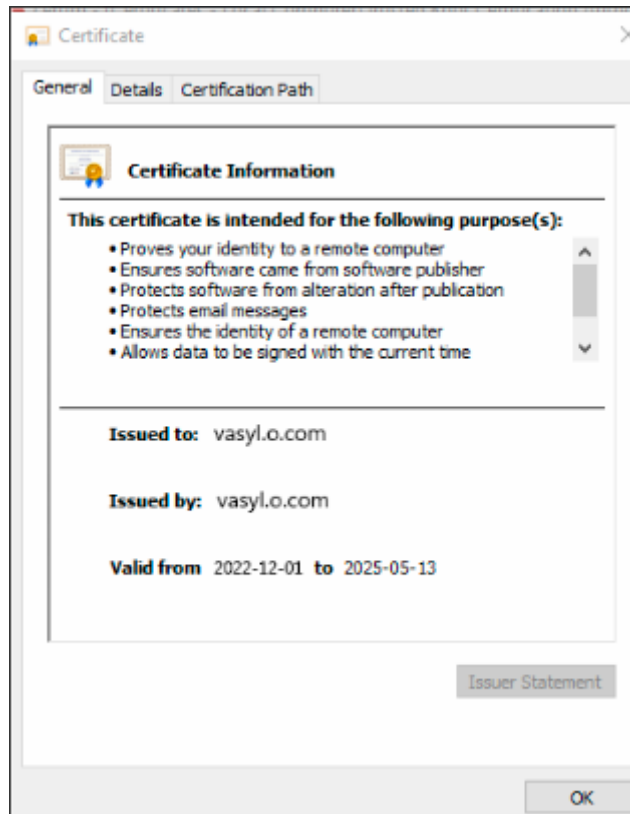


Рис 4 - Довірений сертифікат

```
PS C:\WINDOWS\system32> $cert = New-SelfSignedCertificate -Subject "Cert for Code" -Type CodeSigningCert -CertStoreLocation cert:\LocalMachine\My_
PS C:\WINDOWS\system32> Move-Item -Path $cert.PSPath -Destination "Cert:\CurrentUser\Root"
```

Рис 5 - Створення сертифікату для підпису файлу

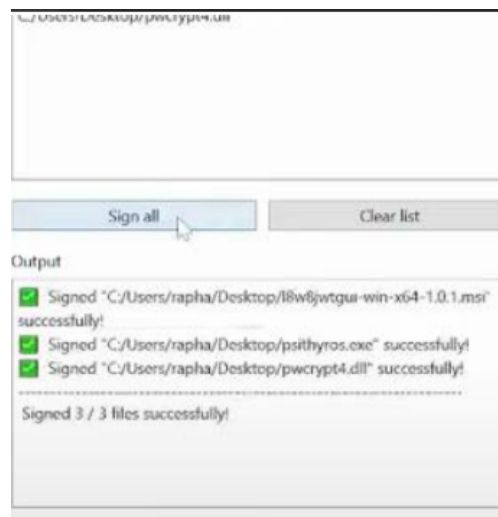


Рис 6 - Підписання програми за допомогою сертифіката

Висновок: під час лабораторної роботи я навчився виконувати файли