

Захист від зміни бінарного файлу

Мета

Навчитися підписувати виконувані файли.

Завдання

- створити сертифікат
- проінсталювати його в систему, щоб він був "довіраним"
- 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

CommandType	Name	Version	Source
-----	----	-----	-----
Cmdlet	Add-CertificateEnrollmentPolicyServer	1.0.0.0	PKI
Cmdlet	Export-Certificate	1.0.0.0	PKI
Cmdlet	Export-PfxCertificate	1.0.0.0	PKI
Cmdlet	Get-Certificate	1.0.0.0	PKI
Cmdlet	Get-CertificateAutoEnrollmentPolicy	1.0.0.0	PKI
Cmdlet	Get-CertificateEnrollmentPolicyServer	1.0.0.0	PKI
Cmdlet	Get-CertificateNotificationTask	1.0.0.0	PKI
Cmdlet	Get-PfxData	1.0.0.0	PKI
Cmdlet	Import-Certificate	1.0.0.0	PKI
Cmdlet	Import-PfxCertificate	1.0.0.0	PKI
Cmdlet	New-CertificateNotificationTask	1.0.0.0	PKI
Cmdlet	New-SelfSignedCertificate	1.0.0.0	PKI
Cmdlet	Remove-CertificateEnrollmentPolicyServer	1.0.0.0	PKI
Cmdlet	Remove-CertificateNotificationTask	1.0.0.0	PKI
Cmdlet	Set-CertificateAutoEnrollmentPolicy	1.0.0.0	PKI
Cmdlet	Switch-Certificate	1.0.0.0	PKI
Cmdlet	Test-Certificate	1.0.0.0	PKI

Рис. 1 – Список доступних командлетів.

```
PS C:\Windows\System32> New-SelfSignedCertificate -DnsName d.n.com -CertStoreLocation cert:\LocalMachine\My

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

Thumbprint                               Subject
-----
32DD6DFE6AE9BBF01DD5C4292977BA54567E4E53  CN=d.n.com

PS C:\Windows\system32>
```

Рис. 2 – Створення сертифікату

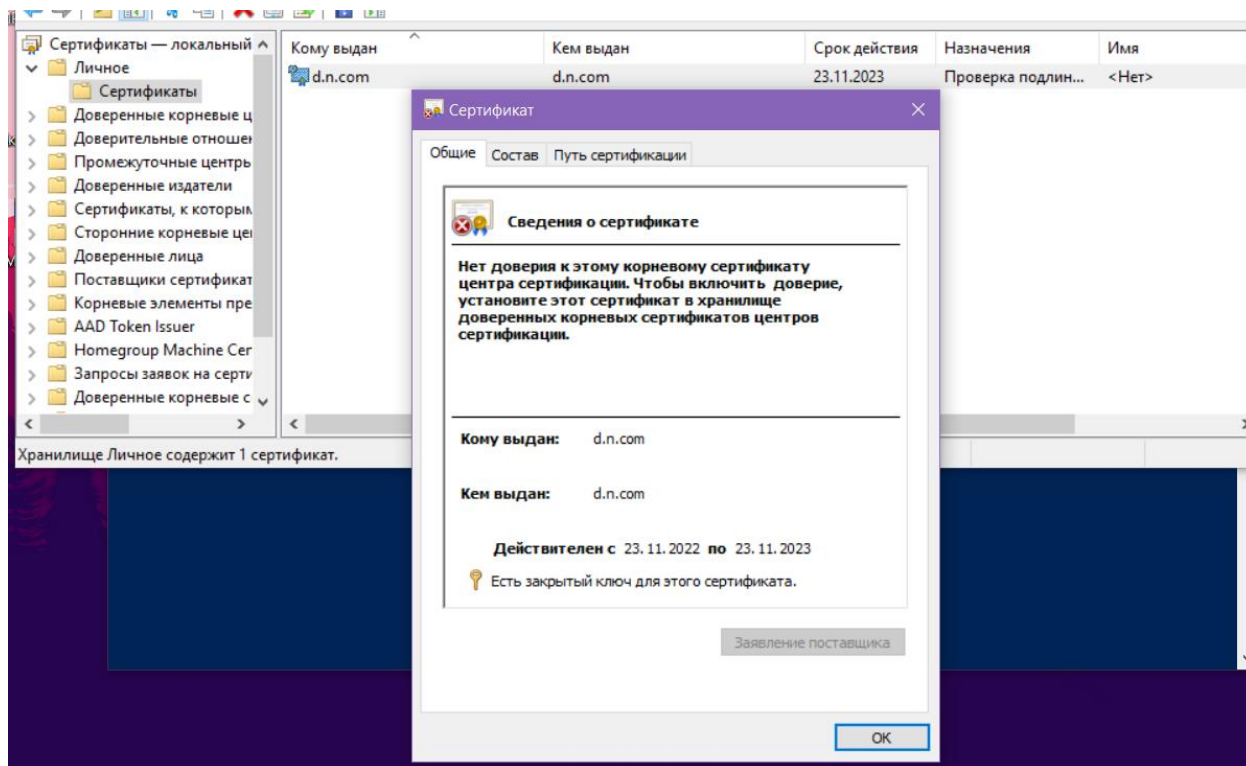


Рис. 3 – Демонстрація того, що сертифікат не довірений.

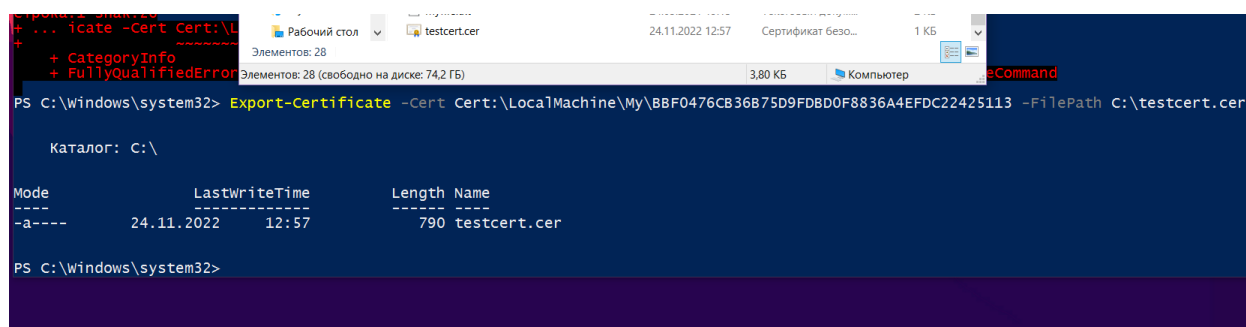


Рис. 4 – Экспорт сертификату на диск та імпорт в довірені сертифікати.

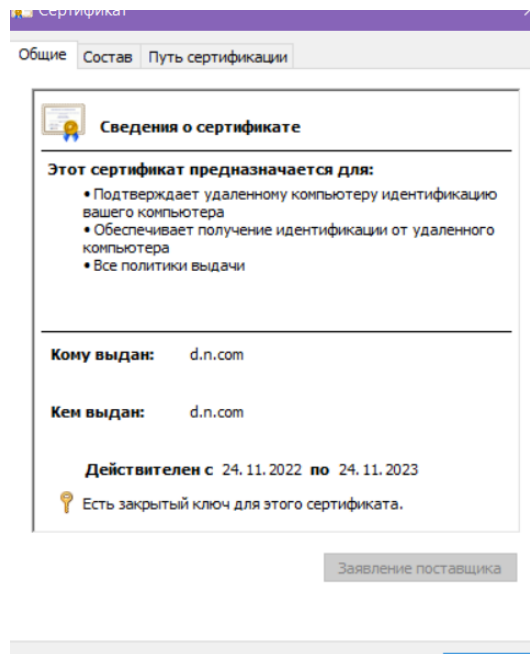


Рис. 5 – Довірений сертифікат.

```
PS C:\Windows\system32> $cert = New-SelfSignedCertificate -Subject "Cert for Code Signing" -Type CodeSigningCert -CertStoreLocation cert:\L
calMachine\My
PS C:\Windows\system32> Move-Item -Path $cert.PSPath -Destination "Cert:\CurrentUser\Root"
```

Рис. 6 – Створення сертифікату для підпису.

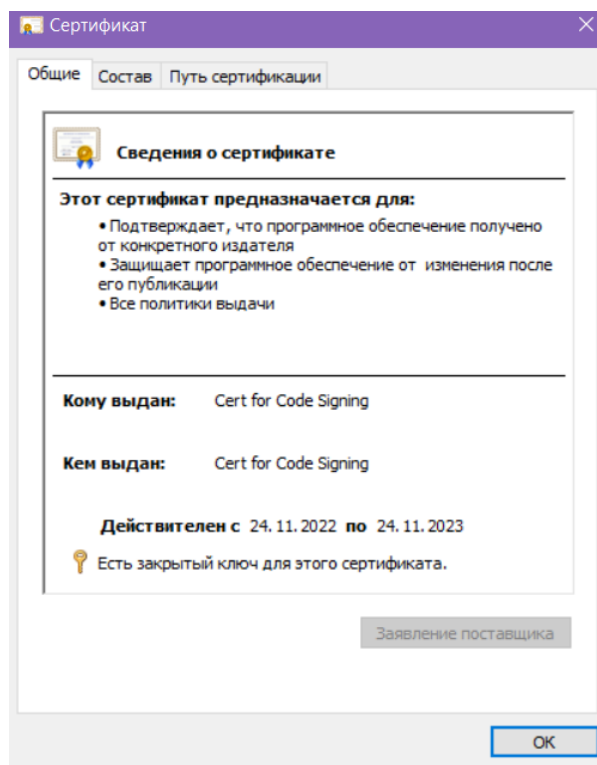


Рис. 7 – Встановлення його в систему (довірення)

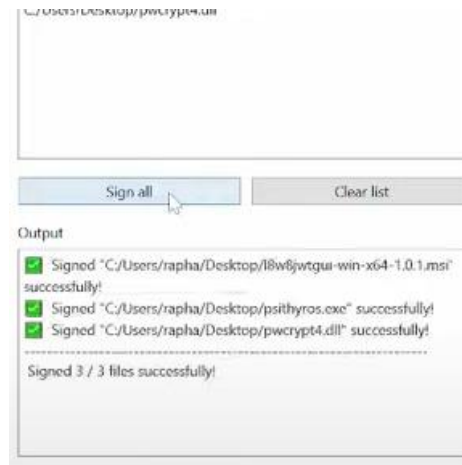


Рис. 8 – Підписання програм за допомогою сертифікату(SignTool GUI).

Висновок : під час лабораторної роботи я навчився підписувати виконувані файли.