

Лабораторна робота №9

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:

```
PS D:\Windows Kits\10\App Certification Kit> New-SelfSignedCertificate -DnsName dan.rud.com -CertStoreLocation "C:\"

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

Thumbprint                               Subject
-----
8D5B995A1139EB67604A39101D8D17FE40C775F6  CN=dan.rud.com

PS D:\Windows Kits\10\App Certification Kit> █
```

Рис. 2 – Створення сертифікату

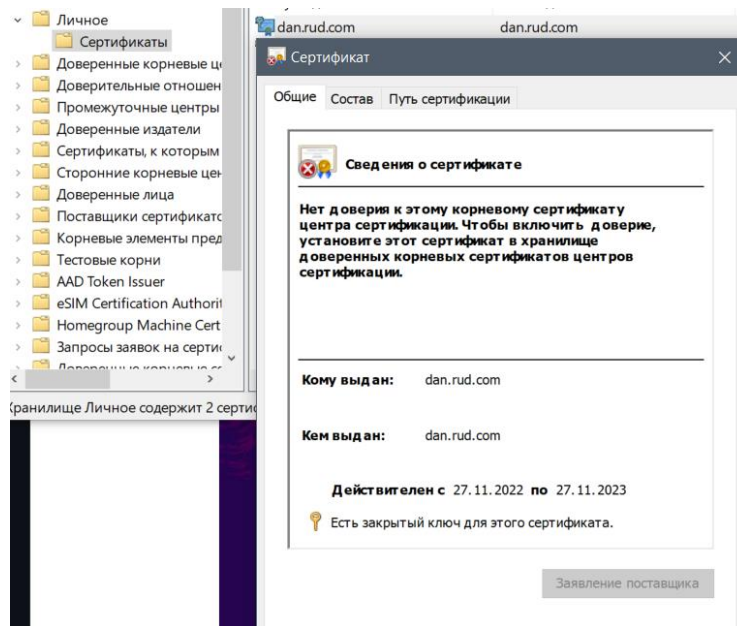


Рис. 2 – Сертификат недовірений

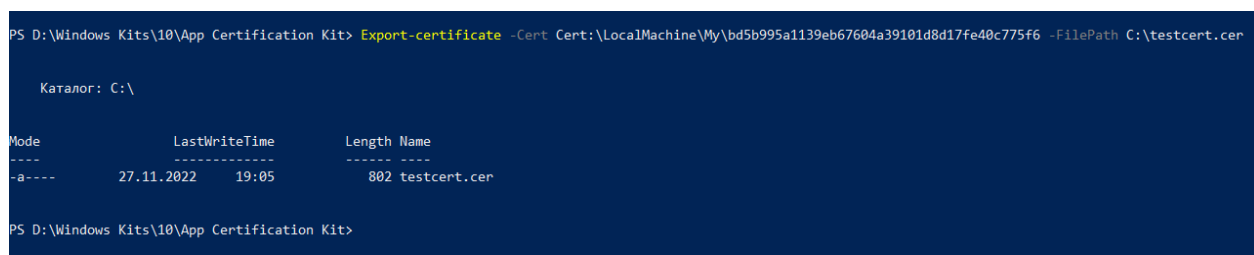


Рис. 3 Экспорт сертификату

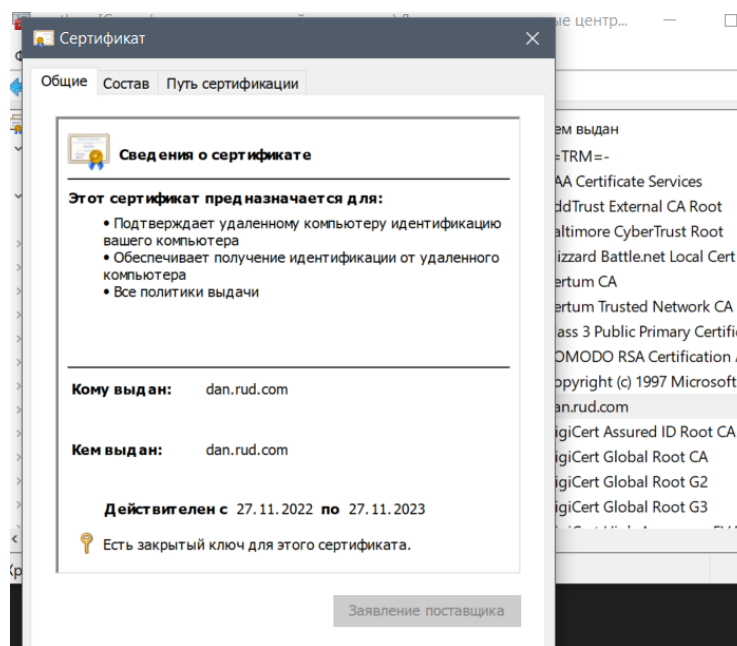
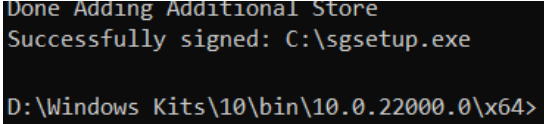


Рис. 4 - Сертифікат довірений (ми імпортували його в довірені, встановили в систему)



```
Done Adding Additional Store  
Successfully signed: C:\sgsetup.exe  
  
D:\Windows Kits\10\bin\10.0.22000.0\x64>
```

Рис. 5 – Підписання програми

Висновок: в результаті виконання лабораторної роботи ми навчилися підписувати виконувані файли.