

## ЗАХИСТ ВІД ЗМІНИ БІНАРНОГО ФАЙЛУ

### Лабораторна робота

**Мета:** Навчитися підписувати виконувані файли.

**Індивідуальне завдання:**

- створити сертифікат
- проінсталювати його в систему, щоб він був "довіреним"
- використовуючи проект будь-якої попередньої роботи, виконати підпис виконаного файлу за допомогою утиліти SignTool (або JarSigner) (інші варіанти повинні бути оговорені з викладачем)
- 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 цілостний

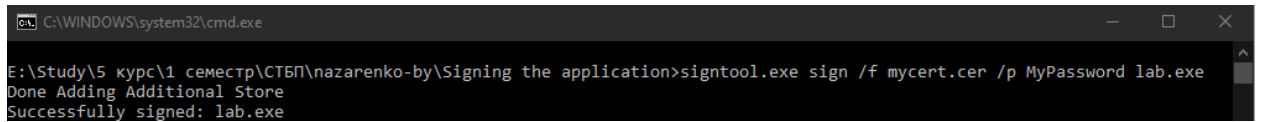
### ХІД РОБОТИ

Підписання коду - це процес цифрового підпису виконуваних файлів і скриптів для підтвердження особи автора програмного забезпечення і гарантії того, що код не був змінений або пошкоджений з моменту його підписання. Публічно довірені сертифікаційні центри (ЦС) підтверджують посвідчення передплатників і пов'язують їх відкритий ключ із сертифікатом підпису коду.

Більшість що продаються сьогодні обчислювальних пристроїв масового ринку поставляються з попередньо завантаженим програмним забезпеченням, але програмне забезпечення, що постачається з пристроєм «з коробки», старіє і часто вимагає оновлення. Для персонального комп'ютера або мобільного пристрою користувачі часто стикаються з ситуаціями, коли їм необхідно завантажити оновлене програмне забезпечення або додаток, Іноді оновлення відбувається в автоматичному режимі. Користувачам рекомендується використовувати додаток на своєму пристрої або відвідуваному їм сайті, щоб, щоб випробувати або використовувати пропоноване їм, їм необхідно оновити,

виправити або розширити свій поточний програмне забезпечення. Їх просять прийняти правильне рішення: «Запустити» або «Не запускати».

Виконаємо підпис попередньої лабораторної роботи за допомогою signtool.



```
C:\WINDOWS\system32\cmd.exe
E:\Study\5 курс\1 семестр\СТБП\nazarenko-by\Signing the application>signtool.exe sign /f mycert.cer /p MyPassword lab.exe
Done Adding Additional Store
Successfully signed: lab.exe
```

Рисунок 1 – Результат підпису

В результаті на рис.2 наведено властивості з підписом файлу.

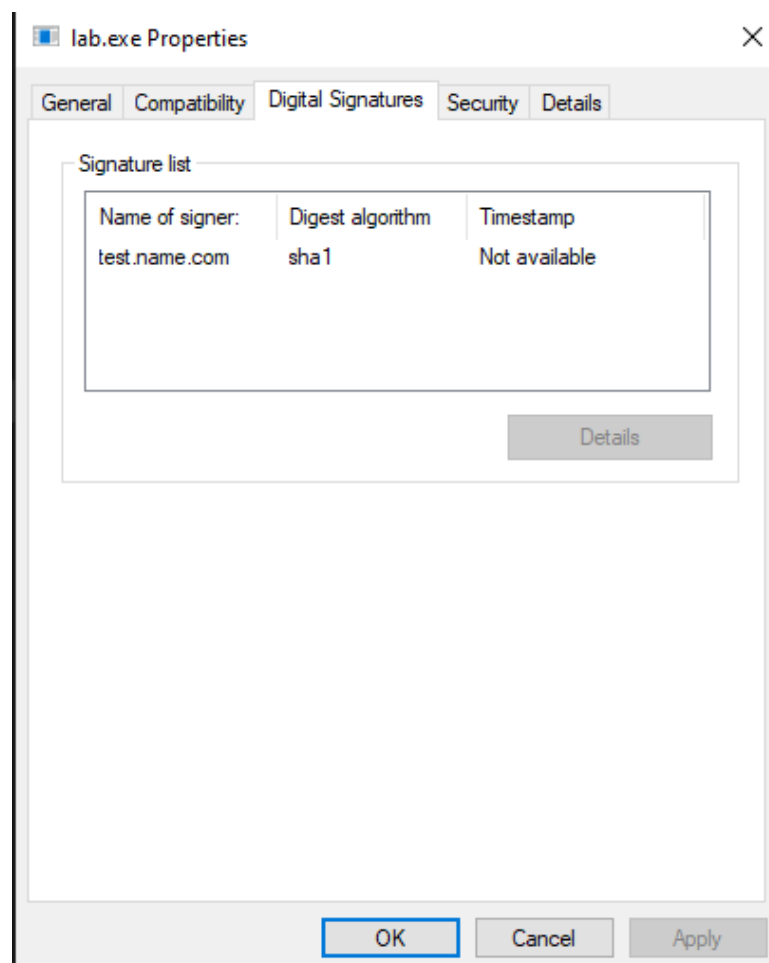


Рисунок 2 – Підпис файлу

Лістинг валідації підпису:

```
int validate(char *certificate, char *url) {
    BIO *certificate_bio = NULL;
    X509 *cert = NULL;
```

```

int valid = 1;

certificate_bio = BIO_new(BIO_s_file());

if (!(BIO_read_filename(certificate_bio, certificate))) {
    fprintf(stderr, "Error in reading cert BIO filename");
    exit(EXIT_FAILURE);
}

if (!(cert = PEM_read_bio_X509(certificate_bio, NULL, 0, NULL))) {
    fprintf(stderr, "Error in loading certificate");
    exit(EXIT_FAILURE);
}

if (validate_dates(cert) == 0 || validate_domain(cert, url) == 0 ||
    validate_key_length(cert) == 0 || validate_key_usage(cert) == 0) {
    valid = 0;
}

X509_free(cert);
BIO_free_all(certificate_bio);
return valid;
}

```

Результат валідації підпису наведено на рис.3.

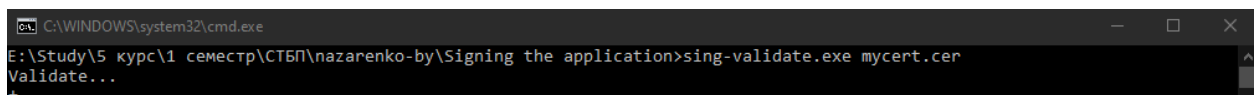


Рисунок 3 – Результат валідації

**Висновки:** в ході лабораторної роботи було отримано навички підпису виконуючих файлів.