Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Лабораторна робота №4

Реалізація
Web-сервісу електронного цифрового підпису
«Easy Digital Sign»
(підгрупа 3А)

в рамках комп’ютерного практикуму
кредитного модуля
«МЕТОДИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ»
бригада «FBDreamTeam»
(ФБ-01мн Вовчановський Павло, Войцеховський Андрій)

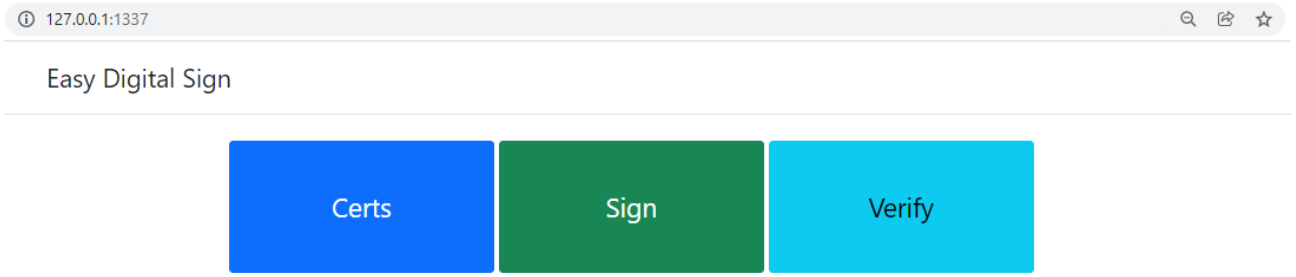
Київ 2021

Технічні характеристики системи

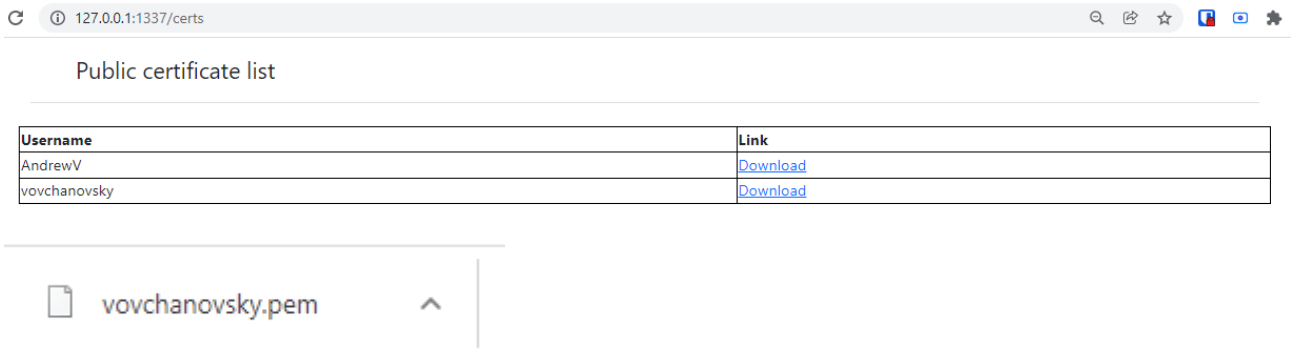
Мова програмування	Python 3
Програмний каркас	Flask
Криптографічна бібліотека сервера	PyCryptodome
Криптографічна бібліотека клієнта	Web Cryptography API
Алгоритм цифрового підпису	RSASSA-PSS
Алгоритм хешування	SHA-256
Формат зберігання ключів	PKCS8
Формат сертифікатів відкритого ключа	X.509

Інтерфейс користувача

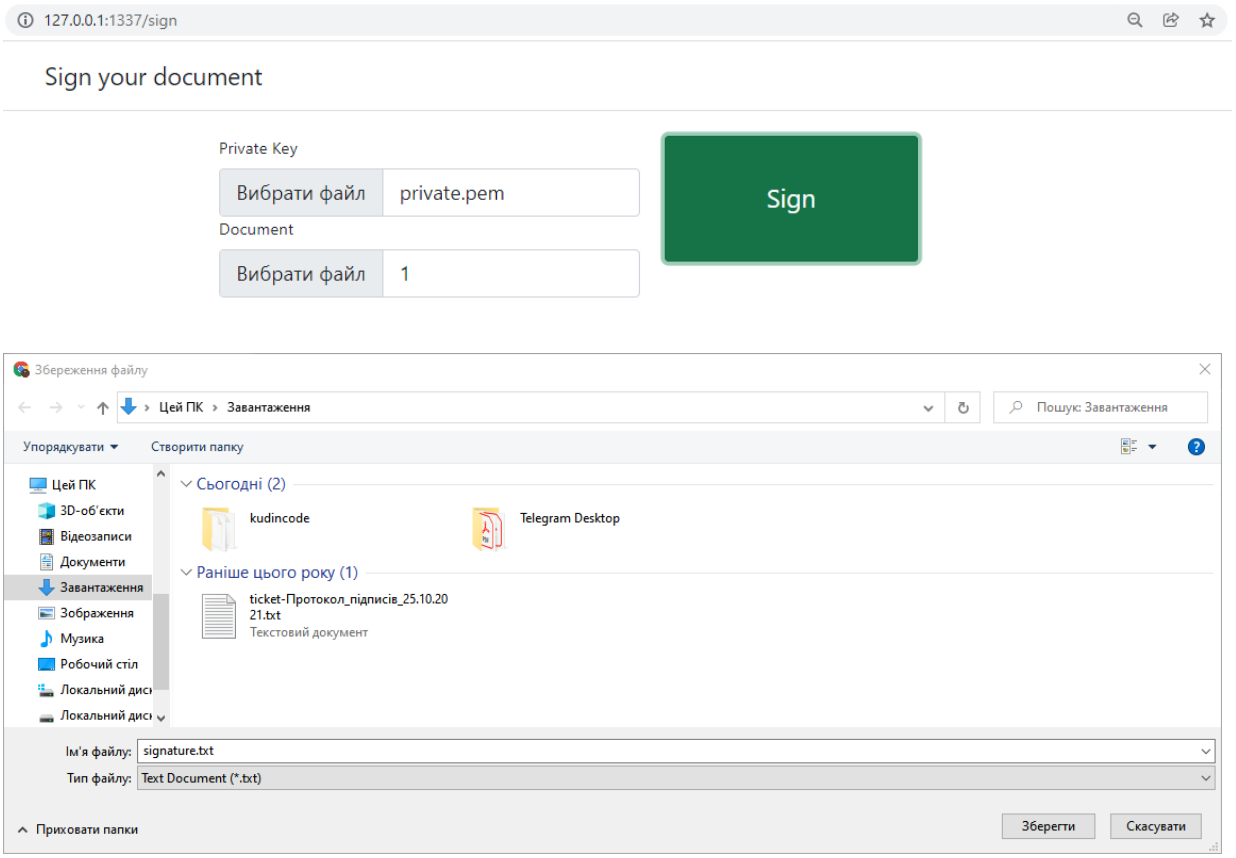
Головна сторінка



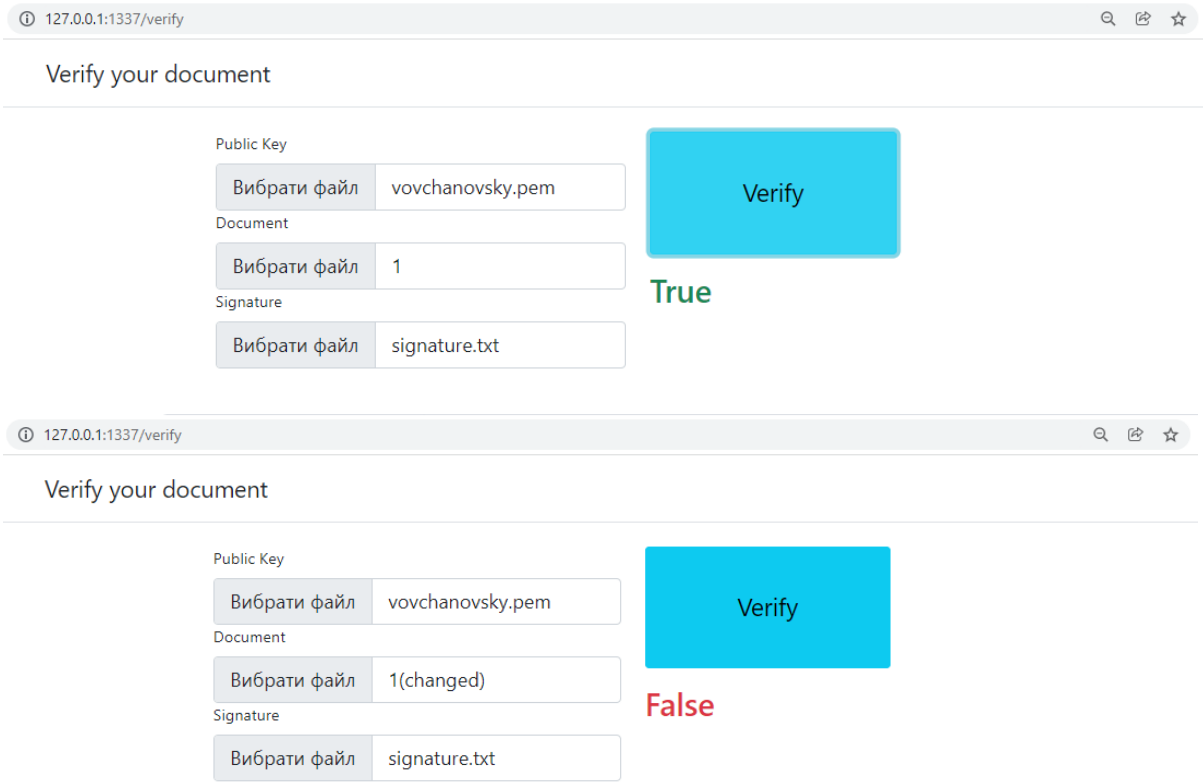
Список сертифікатів відкритого ключа (з опцією завантаження)



Підписання файлів



Перевірка підпису



Додавання сертифікату відкритого ключа до публічного списку (обмежений доступ)