



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»

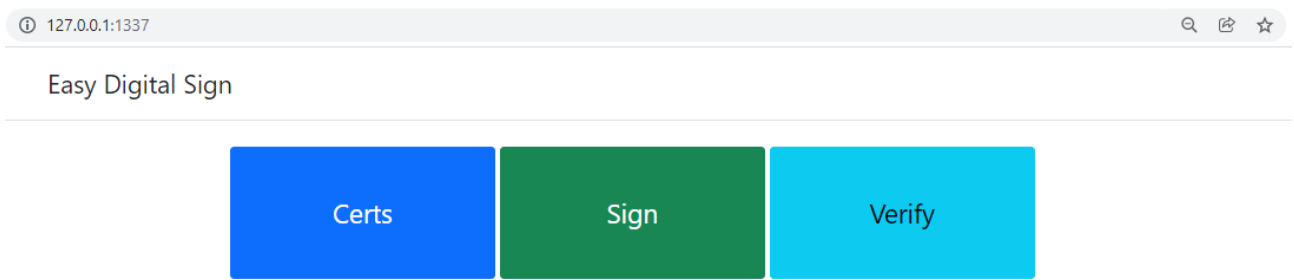
(ФБ-01мн Вовчановський Павло, Войцеховський Андрій)

Технічні характеристики системи

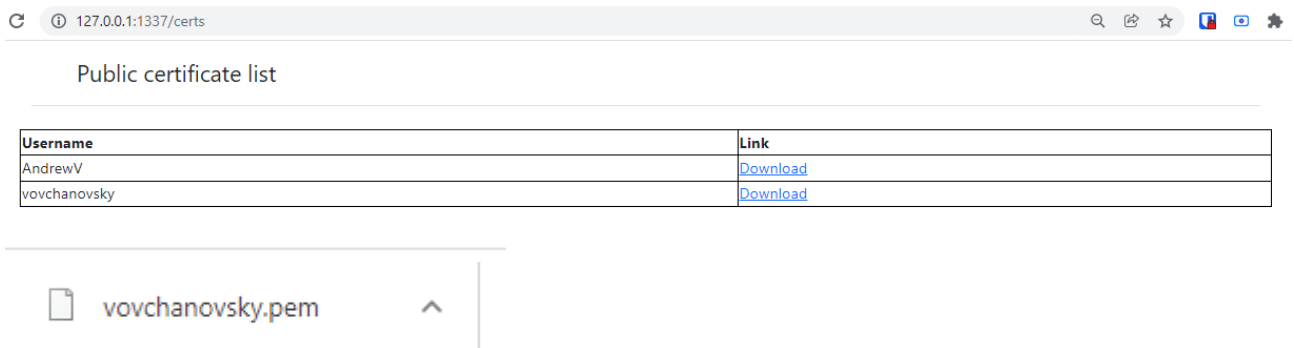
Мова програмування	Python 3
Програмний каркас	Flask
Криптографічна бібліотека сервера	PyCryptodome
Криптографічна бібліотека клієнта	Web Cryptography API
Алгоритм цифрового підпису	RSASSA-PSS
Алгоритм хешування	SHA-256
Формат зберігання ключів	PKCS8
Формат сертифікатів відкритого ключа	X.509

Інтерфейс користувача

Головна сторінка



Список сертифікатів відкритого ключа (з опцією завантаження)



Підписання файлів

127.0.0.1:1337/sign

Sign your document

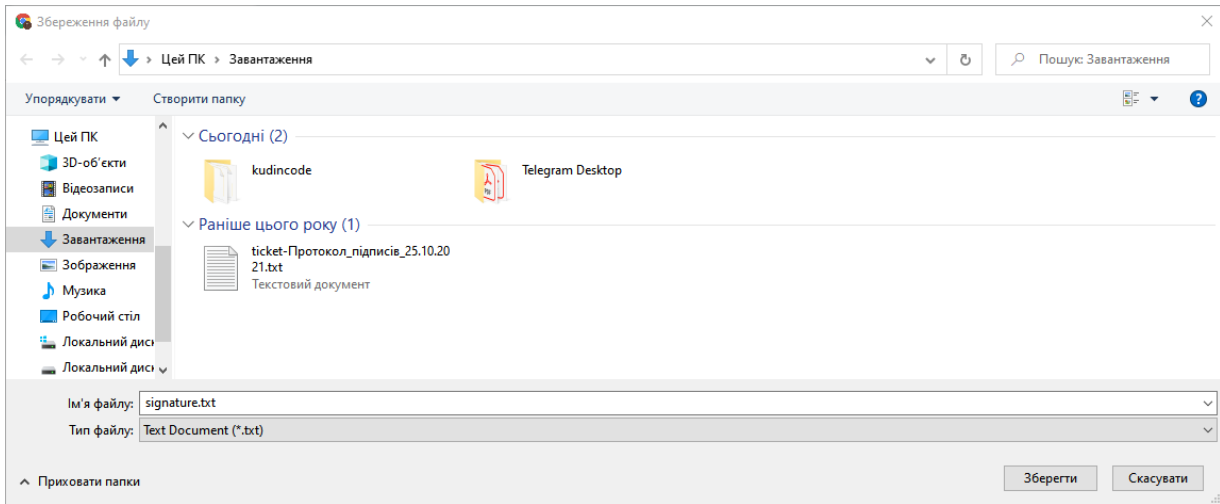
Private Key

Вибрати файл private.pem

Document

Вибрати файл 1

Sign



Перевірка підпису

127.0.0.1:1337/verify

Verify your document

Public Key

Вибрати файл vovchanovsky.pem

Document

Вибрати файл 1

Signature

Вибрати файл signature.txt

Verify

True

127.0.0.1:1337/verify

Verify your document

Public Key

Вибрати файл vovchanovsky.pem

Document

Вибрати файл 1(changed)

Signature

Вибрати файл signature.txt

Verify

False

Додавання сертифікату відкритого ключа до публічного списку (обмежений доступ)

127.0.0.1:1337/addcert

Вхід

http://127.0.0.1:1337

Ім'я користувача

Пароль

Вхід

Скасувати

127.0.0.1:1337/addcert

Add public certs

Username

AndrewV

Cert

Вибрати файл

cert.pem

Завантажити

Certificate list

Username	Link
vovchanovsky	Download