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

Лабораторна робота №2

ТЕХНІЧНЕ ЗАВДАННЯ

на розробку 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

Призначення

Web-сервіс електронного цифрового підпису «Easy Digital Sign» (далі - Сервіс) надає клієнтам наступний функціонал:

- генерація особистих та відкритих ключів електронного цифрового підпису та подання заявки на сертифікацію відкритого ключа
- формування сертифікатів відкритого ключа та внесення до централізованого сховища публічних сертифікатів (далі - ЦСПС)
- надання доступу до сформованих сертифікатів шляхом їх розміщення на Сервісі
- перевірку та підтвердження чинності сертифікатів шляхом надання інформації про їхній статус
- надання користувачам послуг зі створення електронних підписів
- надання користувачам послуг з перевірки електронних підписів
- знищення користувачем протягом строку зберігання особистого ключа шляхом відкликання сертифікату відкритого ключа з ЦСПС

Існуючі аналоги

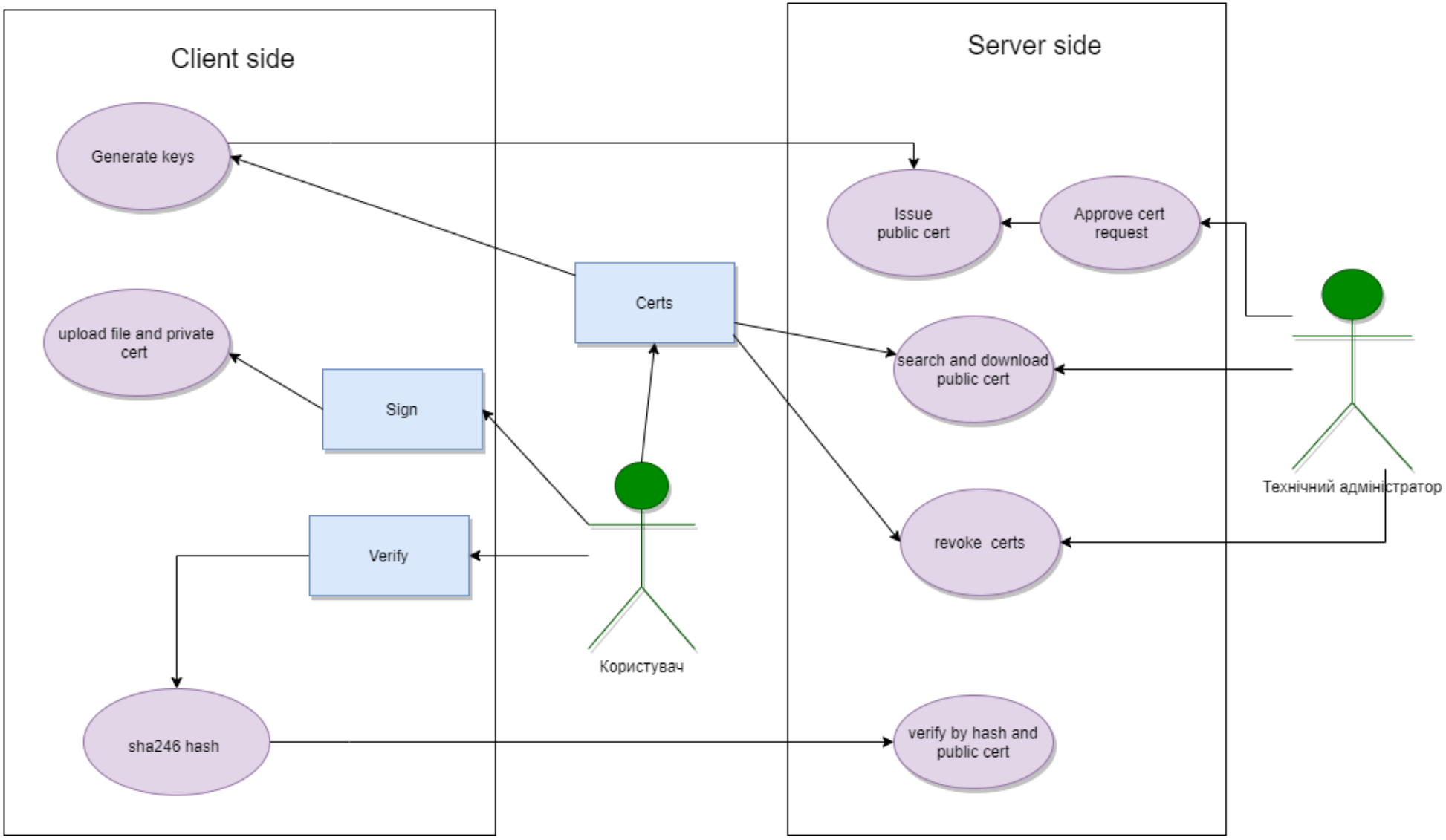
https://sign.diia.gov.ua/

https://acsk.privatbank.ua/certs
https://eu.iit.com.ua/sign-agent/index.html

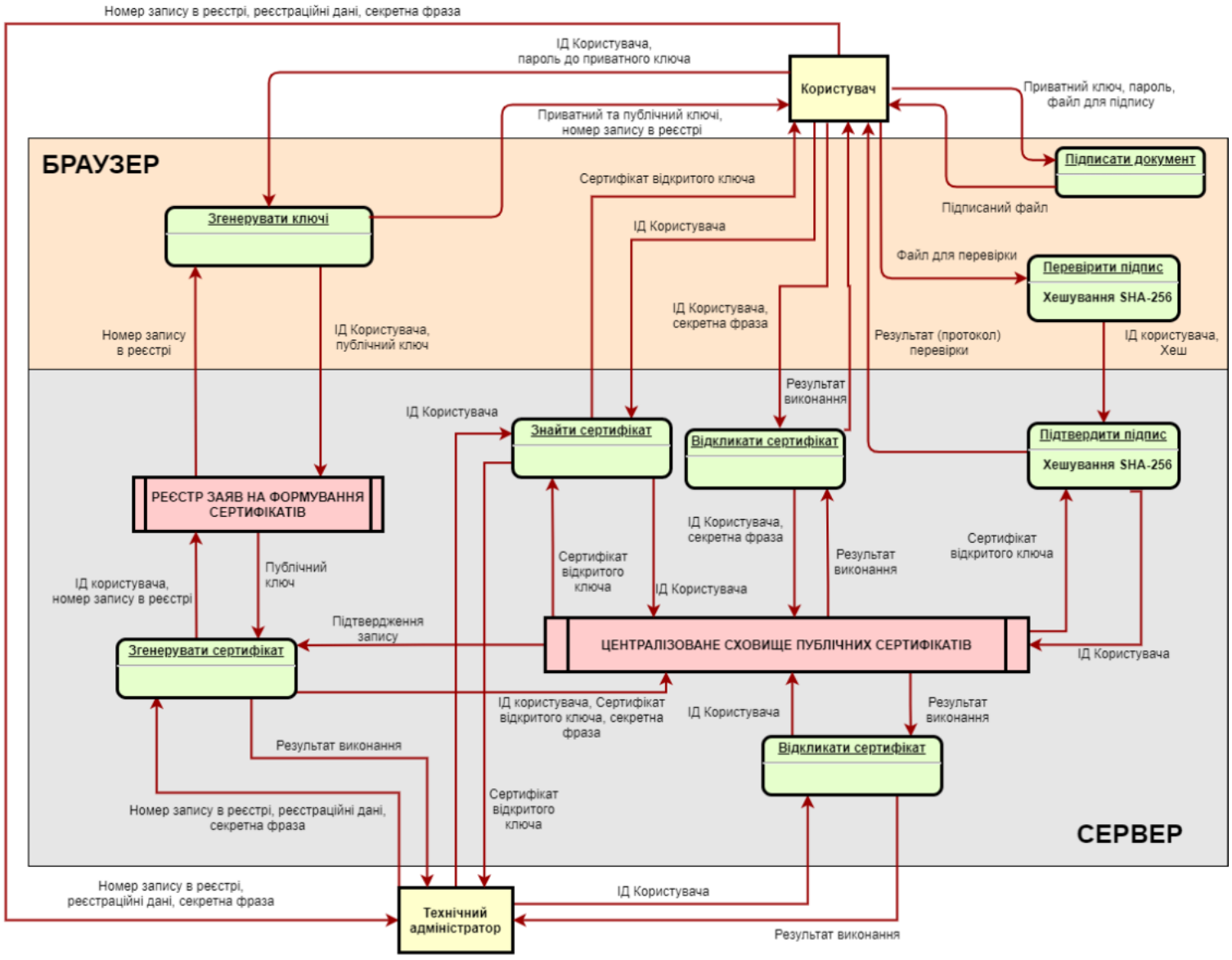
Технічні вимоги до системи

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

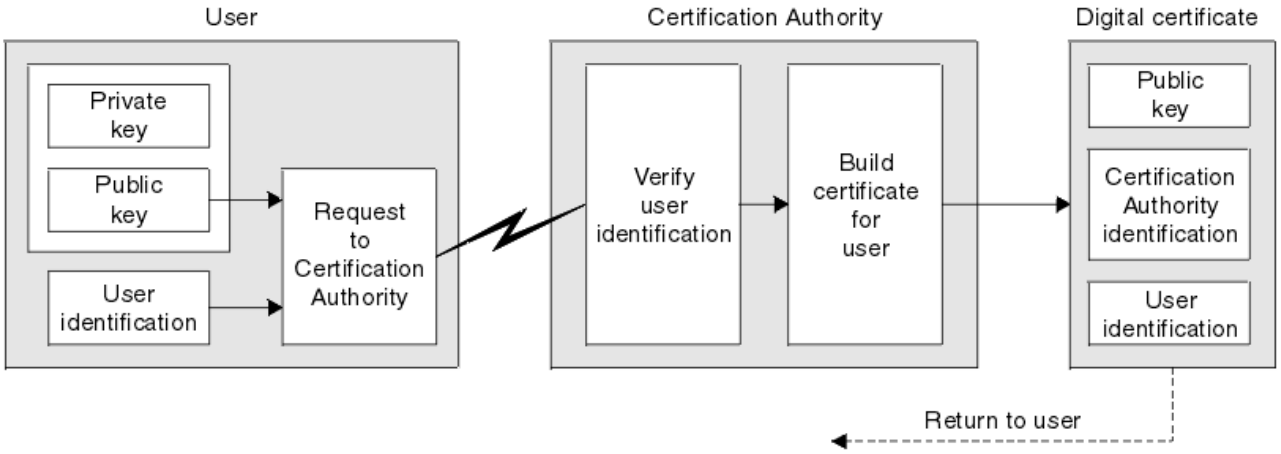
UML діаграма



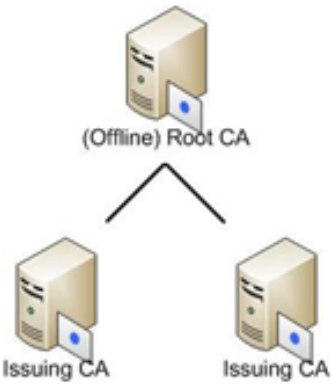
DFD (Діаграма потоків даних)

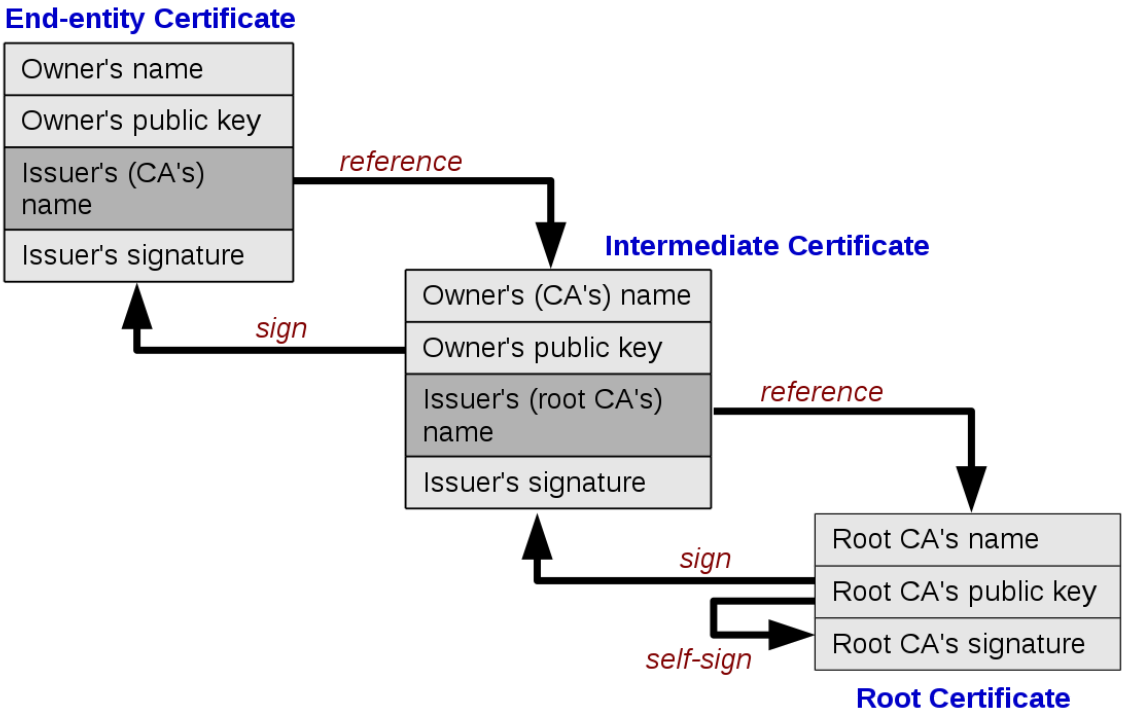


PKI (Інфраструктура відкритих ключів)



Дворівнева ієрархія CA





Функціональні вимоги

Три кнопки на головній сторінці: «Certs» (Меню керування сертифікатами), «Sign» (Підписання файлів), «Verify» (Перевірка підпису)

Certs (Меню керування сертифікатами)

- «Create cert» (Формування заявки на отримання сертифікату): отримання реєстраційних даних від користувача→генерація особистого та відкритого ключів→надсилання клієнту відповідних ключових та формування заявки на отримання сертифікату відкритого ключа
- «Search cert» (Пошук сертифікату по реєстраційним даним особи (ІПН) відкритого ключа в ЦСПС, у разі успіху - можливість завантаження цього ключа та сертифікату до нього).
- «Revoke cert» (Відкликання сертифікату шляхом введення реєстраційних даних особи та ключової фрази)
- Генерація сертифікатів відкритого ключа технічним адміністратором

Sign(Підписання файлів)

- Формування підпису , можливість завантаження файлу та сертифікату

Verify(Перевірка підписаних файлів)

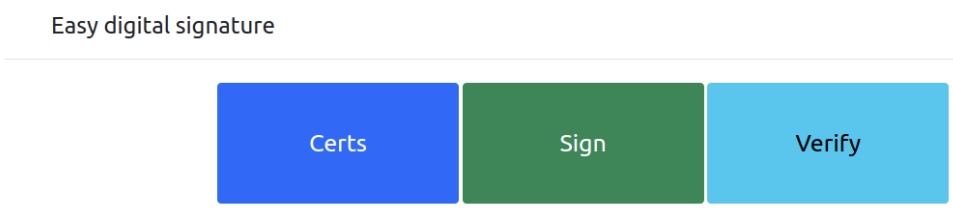
- завантаження підписаного файлу, виведення результату перевірки

Панель технічного адміністратора:

- пошук заявок та формування сертифікатів відкритого ключа, збереження їх в ЦСПС
- пошук та завантаження публічних сертифікатів
- відкликання сертифікатів в ЦСПС

Інтерфейс користувача

Головна сторінка



Підпис на стороні клієнта