НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ім. І.Сікорського"

Дипломна робота магістра
на тему:

«Система авторизації мікросервісів на основі KeyCloak для захисту середовищ хмарних обчислень»

Виконав:
студент 6-го курсу гр. ТР-71мп Прижков А.О.
Керівник:
к.т.н. доцент Смаковський Д.С.

Київ – 2018

Метою дослідження є створення фреймворку для вирішення задачі авторизації користувачів у системах хмарних обчислень з мікросервісною архітектурою.

Об’єктом дослідження є проблема авторизація користувачів у системах хмарних обчислень з мікросервісною архітектурою .

Предметом дослідження є авторизація користувачів у системах хмарних обчислень з мікросервісною архітектурою.

Наукова новизна одержаних результатів.

Найбільш суттєвими науковими результатами магістерської дисертації є вирішення проблеми авторизації користувачів у системах хмарних обчислень з мікросервісною архітектурою

Практичне значення одержаних результатів

Практичне значення одержаних результатів роботи полягає в розробка фреймворку, що вирішує проблему авторизації користувачів у системах хмарних обчислень з мікросервісною архітектурою.

Актуальність теми

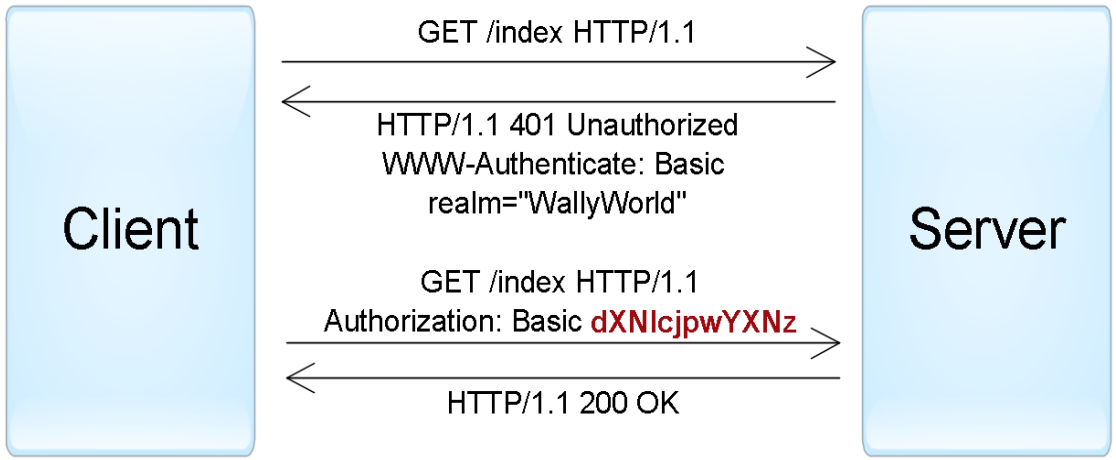
- Мікросервісна архітектура здобуває все більшу популярність, адже вона надає ряд переваг порівняно з монолітною архітектурою, а саме: підтримувати невеликі сервіси легше; можливість горизонтального масштабування; краща відмовостійкість коду; незалежність вибору технологій для кожного з сервісів. Проте, цей підхід має і недоліки, один з таких – спосіб авторизації - для мікросервісів необхідно використовувати аутентифікацію користувача лише по токенах, адже потрібно передавати цей токен між усіма мікросервісами. Це створює проблему для роботи з середовищами хмарних обчислень, адже для них зазвичай використовують аутентифікацію по ключам-доступам (наприклад, найпопулярніше хмарне середовище Amason Web Service використовує саме цей тип). Отже, постає проблема, що нам потрібно розробити додатковий функціонал, який буде поєднувати ці два методи аутентифікації.

1. СУЧАСНІ МЕТОДИ АВТОРИЗАЦІЇ КОРИСТУВАЧІВ

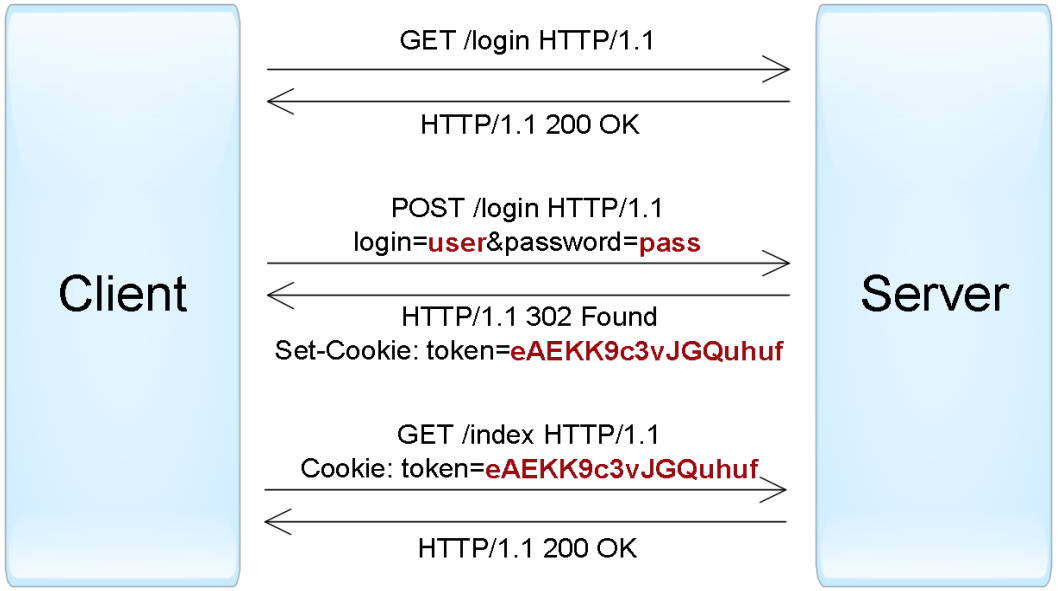
1.1. Аутентифікація по паролю

Цей метод грунтується на тому, що користувач повинен надати username і password для успішної ідентифікації і авторизації в системі.

- Basic аутентифікація



- Forms аутентифікація

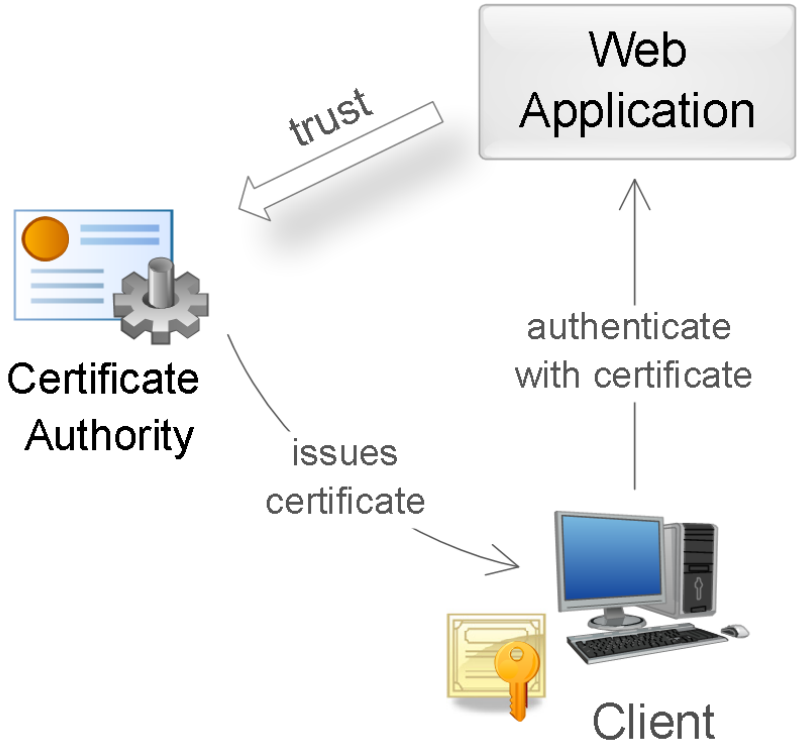


1. СУЧАСНІ МЕТОДИ АВТОРИЗАЦІЇ КОРИСТУВАЧІВ

1.2. Аутентифікація по сертифікатам

Сертифікат являє собою набір атрибутів, що ідентифікують власника. Certificate authority (CA) гарантує справжність сертифікатів.

- Під час аутентифікації сервер виконує перевірку сертифіката на підставі наступних правил:
- Сертифікат повинен бути підписаний довіреною certification authority (перевірка ланцюжка сертифікатів);
- Сертифікат повинен бути дійсним на поточну дату (перевірка терміну дії);
- Сертифікат не повинен бути відкликаний відповідним CA (перевірка списків виключення).

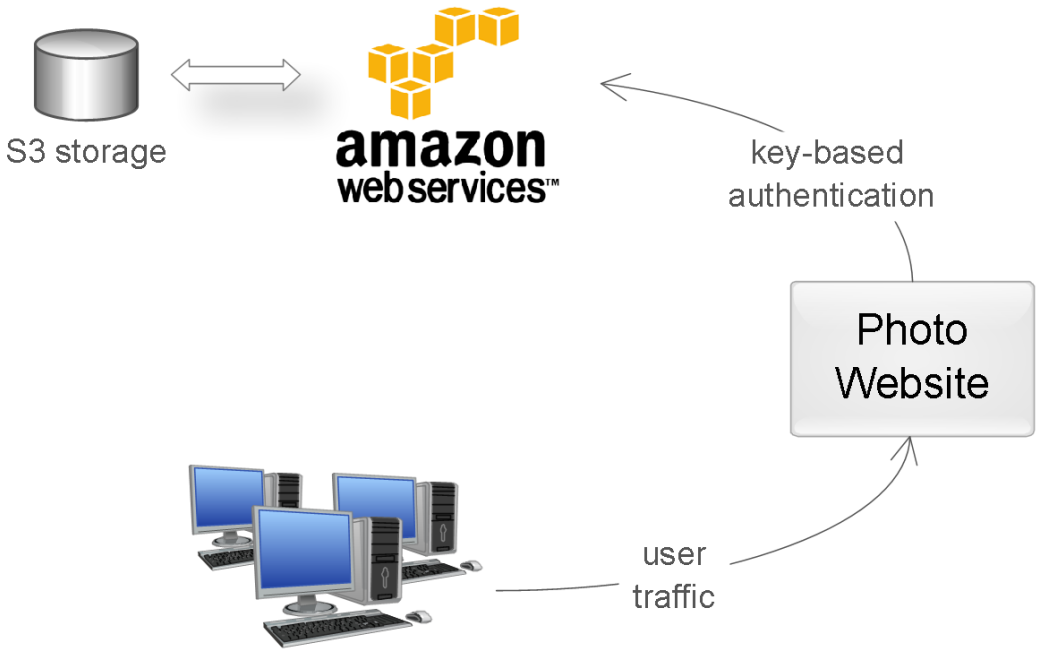


1. СУЧАСНІ МЕТОДИ АВТОРИЗАЦІЇ КОРИСТУВАЧІВ

1.3. Аутентифікація по ключам доступу

- Тут в якості секрету застосовуються ключі доступу (access key, API key) - довгі унікальні рядки, що містять довільний набір символів, по суті замінюють собою комбінацію username / password.

- У більшості випадків, сервер генерує ключі доступу за запитом користувачів, які далі зберігають ці ключі в клієнтських додатках. При створенні ключа також можливо обмежити термін дії і рівень доступу, який отримає клієнтська програма при аутентифікації за допомогою цього ключа.

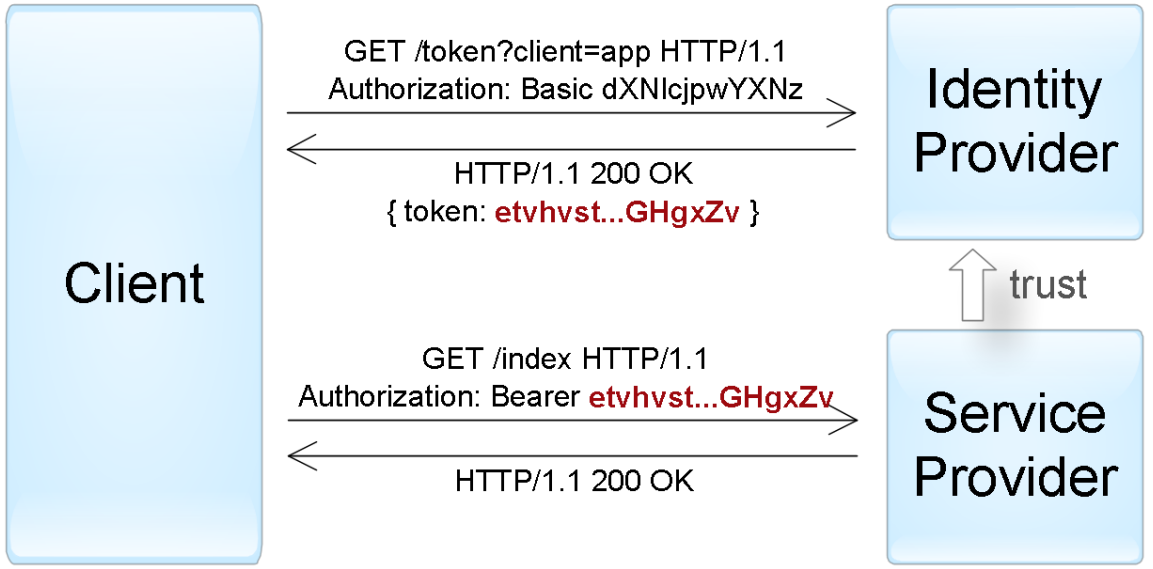


1. СУЧАСНІ МЕТОДИ АВТОРИЗАЦІЇ КОРИСТУВАЧІВ

1.4. Аутентифікація по токенах

- Найчастіше застосовується при побудові розподілених систем Single Sign-On (SSO), де один додаток (service provider або relying party) делегує функцію аутентифікації користувачів іншому додатку (identity provider або authentication service).

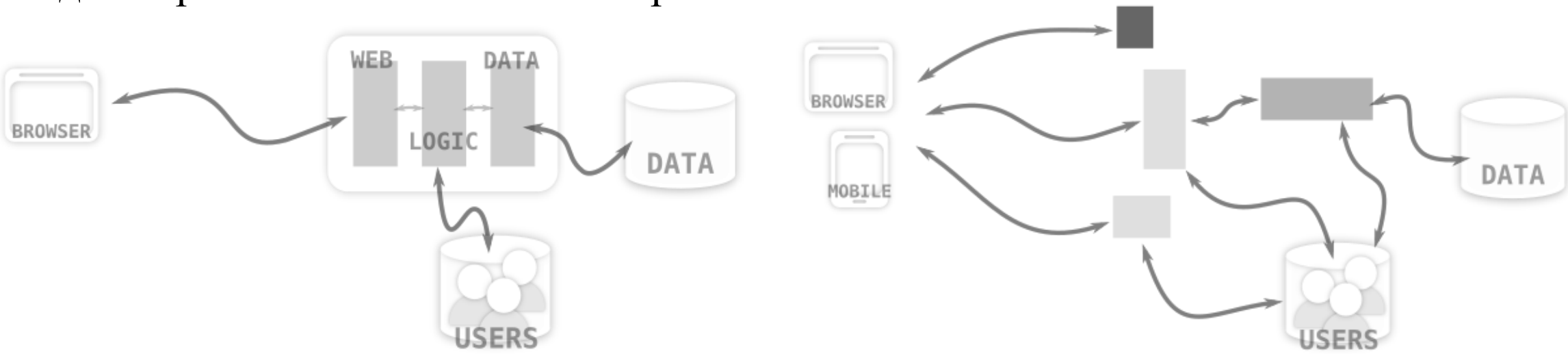
- На загальному рівні, весь процес виглядає наступним чином:
- клієнт аутентифікується в identity provider одним із способів, специфічним для нього (пароль, ключ доступу, сертифікат, ітд.);
- клієнт просить identity provider надати йому токен для конкретного SP-додатки. Identity provider генерує токен і відправляє його клієнту;
- клієнт аутентифікується в SP-додатку за допомогою цього токена.



2. АВТОРИЗАЦІЯ КОРИСТУВАЧІВ У СИСТЕМАХ ХМАРНИХ ОБЧИСЛЕНЬ З МІКРОСЕРВІСНОЮ АРХІТЕКТУРОЮ

2.1. Авторизацію користувачів у мікросервісній архітектурі

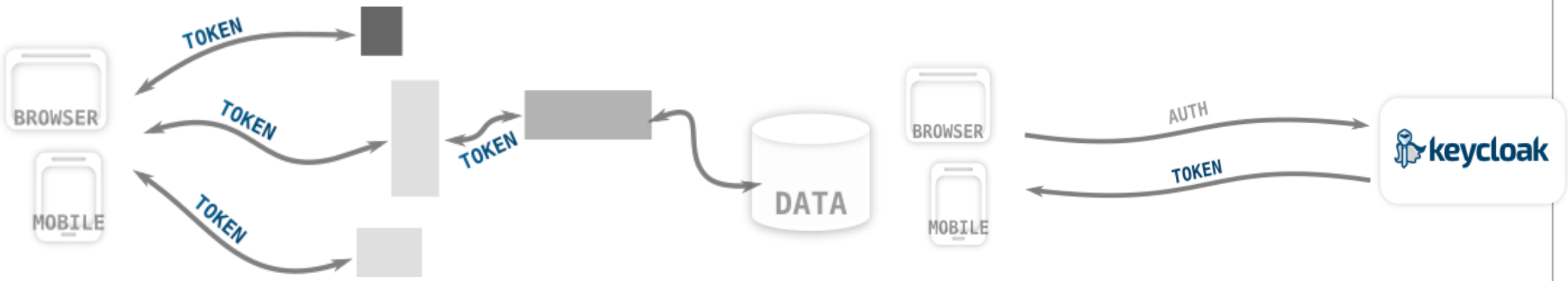
- Архітектурний стиль мікросервісов — це підхід, при якому єдине додаток будується як набір невеликих сервісів, кожен з яких працює у власному процесі і взаємодіє з іншими використовуючи легкі механізми (HTTP);
- Аутентифікація користувачів у системах з мікросервісною архітектурою відбувається лише на основі токенів, адже незалежність сервісів один від одного робить неможливим використання сесій



2. АВТОРИЗАЦІЯ КОРИСТУВАЧІВ У СИСТЕМАХ ХМАРНИХ ОБЧИСЛЕНЬ З МІКРОСЕРВІСНОЮ АРХІТЕКТУРОЮ

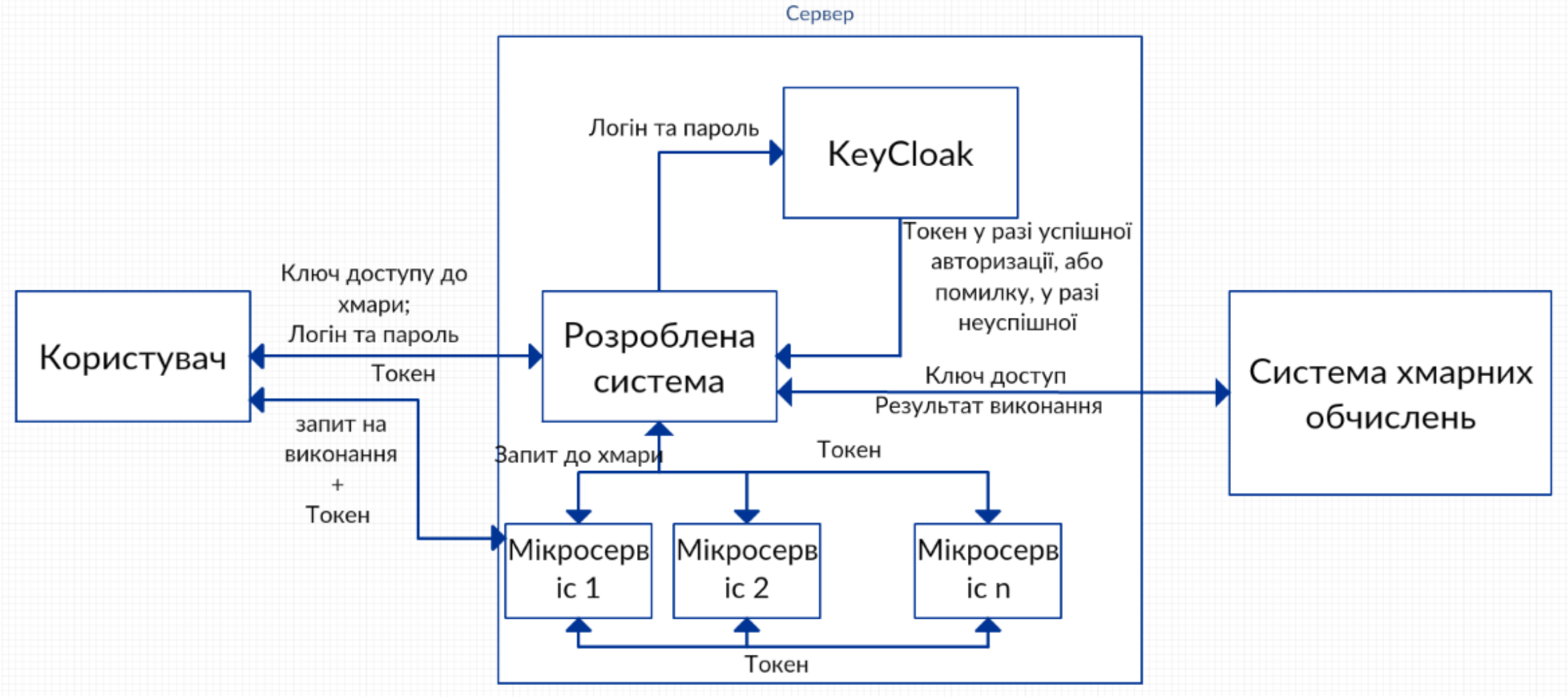
2.1. Сервіс авторизації KeyCloak

- Оскільки мікросервіси — це набір малих сервісів, кожен з яких вирішує одне конкретне завдання, очевидним рішенням безпеки є служба аутентифікації та авторизації. У розробленій системі було використона у якості сервісу авторизації KeyCloak.



2. АВТОРИЗАЦІЯ КОРИСТУВАЧІВ У СИСТЕМАХ ХМАРНИХ ОБЧИСЛЕНЬ З МІКРОСЕРВІСНОЮ АРХІТЕКТУРОЮ

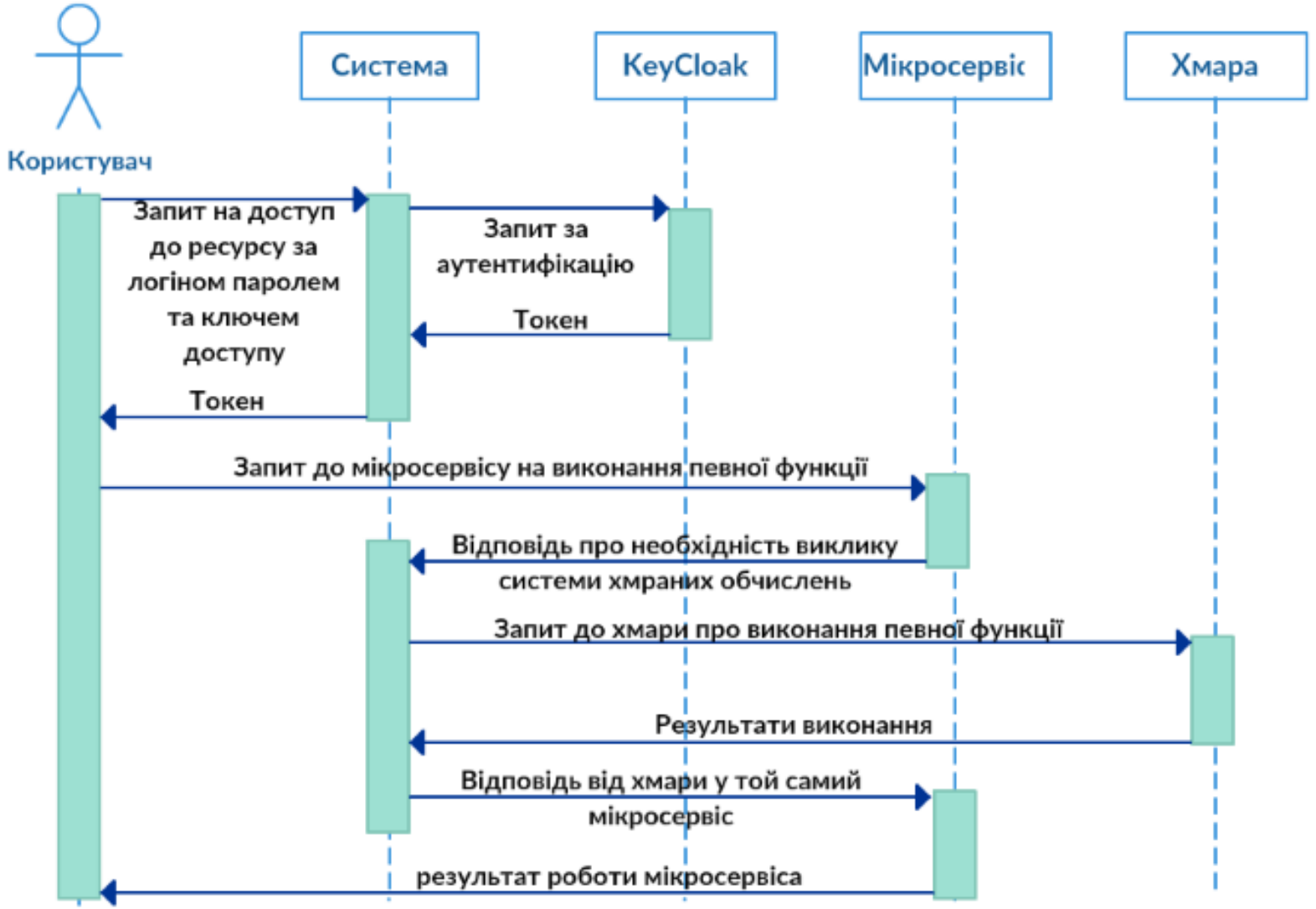
2.3. Фреймворк для авторизації в системах хмарних обчислень з мікросервісною архітектурою



3. РОЗРОБКА ФРЕЙМВОРКУ ДЛЯ АВТОРИЗАЦІЯ КОРИСТУВАЧІВ У СИСТЕМАХ ХМАРНИХ ОБЧИСЛЕНЬ З МІКРОСЕРВІСНОЮ АРХІТЕКТУРОЮ

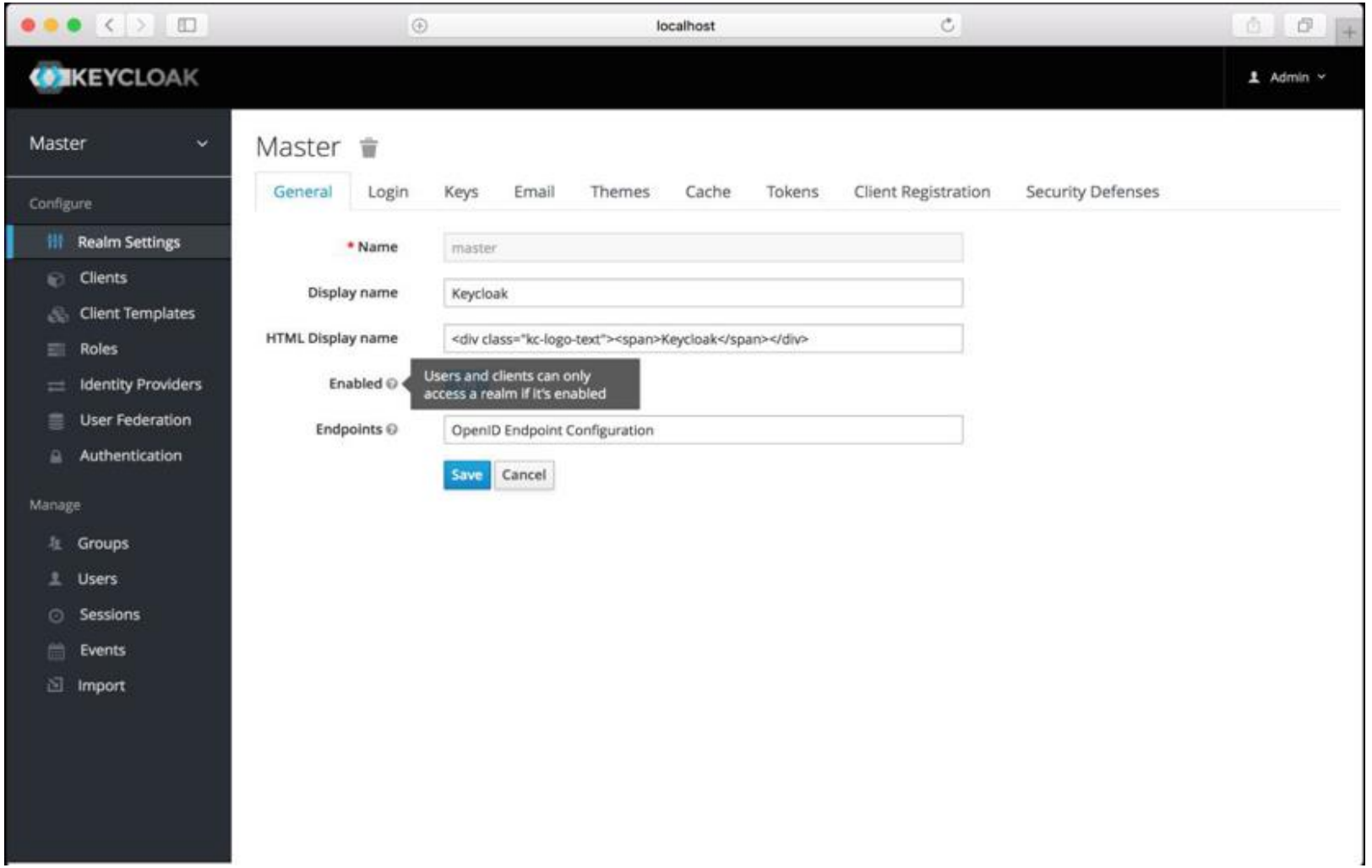
Вибір засобів реалізації системи

3.2. Опис програмної реалізації системи



4. МЕТОДИКА РОБОТИ КОРИСТУВАЧА З ПРОГРАМНОЮ СИСТЕМОЮ

4.1. Інтерфейс KeyCloak



5. Розроблення стартап проекту

- Цільова аудиторія розробленої системи: програмісти;
- Умови для реалізації стартапу на ринку оцінено як сприятливі;
- Прямих конкурентів на ринку не виявлено.

Маркетингова програма має бути побудована наступним чином:

- Розробка функціоналу програмного застосунку;
- Аналіз затребуваності товару на ринку та визначення цільової аудиторії;
- За базову стратегію розвитку необхідно використати стратегію диференціації, яка передбачає, що конкурентноспроможність продукту досягається шляхом, що продукт має якнайкраще відповідати потребам споживачів, що в свою чергу досягається ретельним вивченням ринку. Споживацька цікавість має досягатися завдяки одній або декільком відмінних та інноваційних характеристик;
- Стратегія конкурентної поведінки передбачає використання стратегії лідера, тобто розроблений застосунок орієнтується на всіх ймовірних споживачів на споживчому ринку, у тому числі і клієнтів конкуруючих фірм. Основною цілю є закріплення на ринку та згодом випередження лідерів обраного сегменту.

ВИСНОВКИ

При вирішенні поставлених задач отримані наступні результати:
1. На основі аналізу сучасних методів аутентифікації було виявлено, що безпосередня авторизація у програмах з мікросервісною архітектурою у системах хмарних обчислень неможлива.
2. Аналіз програмних комплексів для авторизації показав, що не існує програмних засобів, які дозволяють використовувати мікросервісну архітектуру для роботи з системами хмарних обчислень.
3. Було проаналізовано архітектуру мікросервісів і на основі цих даних розроблено концепт реалізації ідеї взаємодії їх з системами хмарних обчислень.
4. Розроблено архітектуру підходу для подолання проблеми авторизації.

ВИСНОВКИ

5. Проаналізовано та обрано засоби реалізації для створенні програмного забезпечення.
6. Розроблено систему авторизації користувачів у системах хмарних обчислень з мікросервісною архітектурою
7. На основі поданої ідеї було розроблено бізнес-стартап проекту. Був проведений технологічний аудит, проведено аналіз ринкових можливостей, розроблена базова стратегія розвитку програмного продукту, маркетингова програма, стратегія конкурентної поведінки на ринку, розглянуто перспективи впровадження з огляду на потенційні групи користувачів програмного продукту.
8. Подальші дослідження можуть бути спрямовані на розширення функціоналу запропонованого рішення.

АПРОБАЦІЯ РЕЗУЛЬТАТІВ

Основні положення роботи доповідались і обговорювались на :

1. Сталий розвиток – XXI століття: управління, технології, моделі Дискусії 2018; колективна монографія, м.Київ, 2018р
2. XVI міжнародна науково-практична конференція аспірантів, магістрантів, студентів «Сучасні проблеми наукового забезпечення енергетики» (м. Київ, 26-27 квітня 2018 року).