РОЗРОБКА СИСТЕМИ ЄДИНОГО ВХОДУ

Виконав студент групи ПІ-16м Щепілов Назар Сергійович

Науковий керівник к.т.н., доц. каф. ПЗ Коваленко Олена Олексіївна

Актуальність роботи

service service mobile ...n

Актуальність роботи – Система єдиноко входу покращую досвід користувачів та зменшує кількість мість зберігання паролю .

Мета

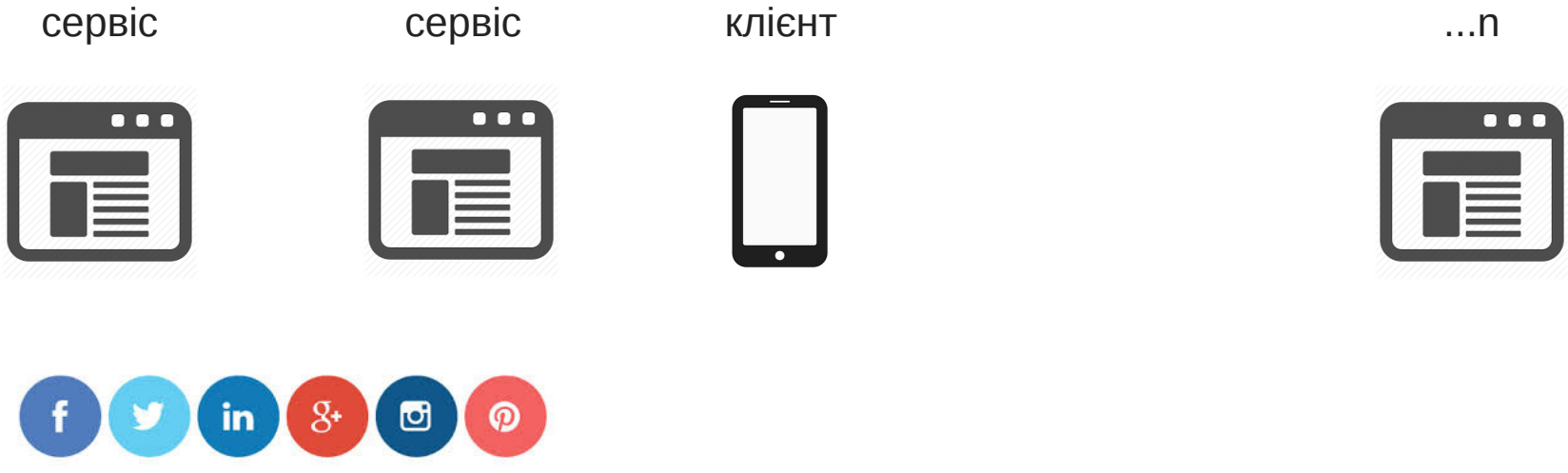
Мета виконання дипломної роботи – є створення системи єдиного входу, що забезпечить безпечне зберігання паролів, та покращить взаємодію із клієнтами, за рахунок спрощення авторизації між різними сервісами

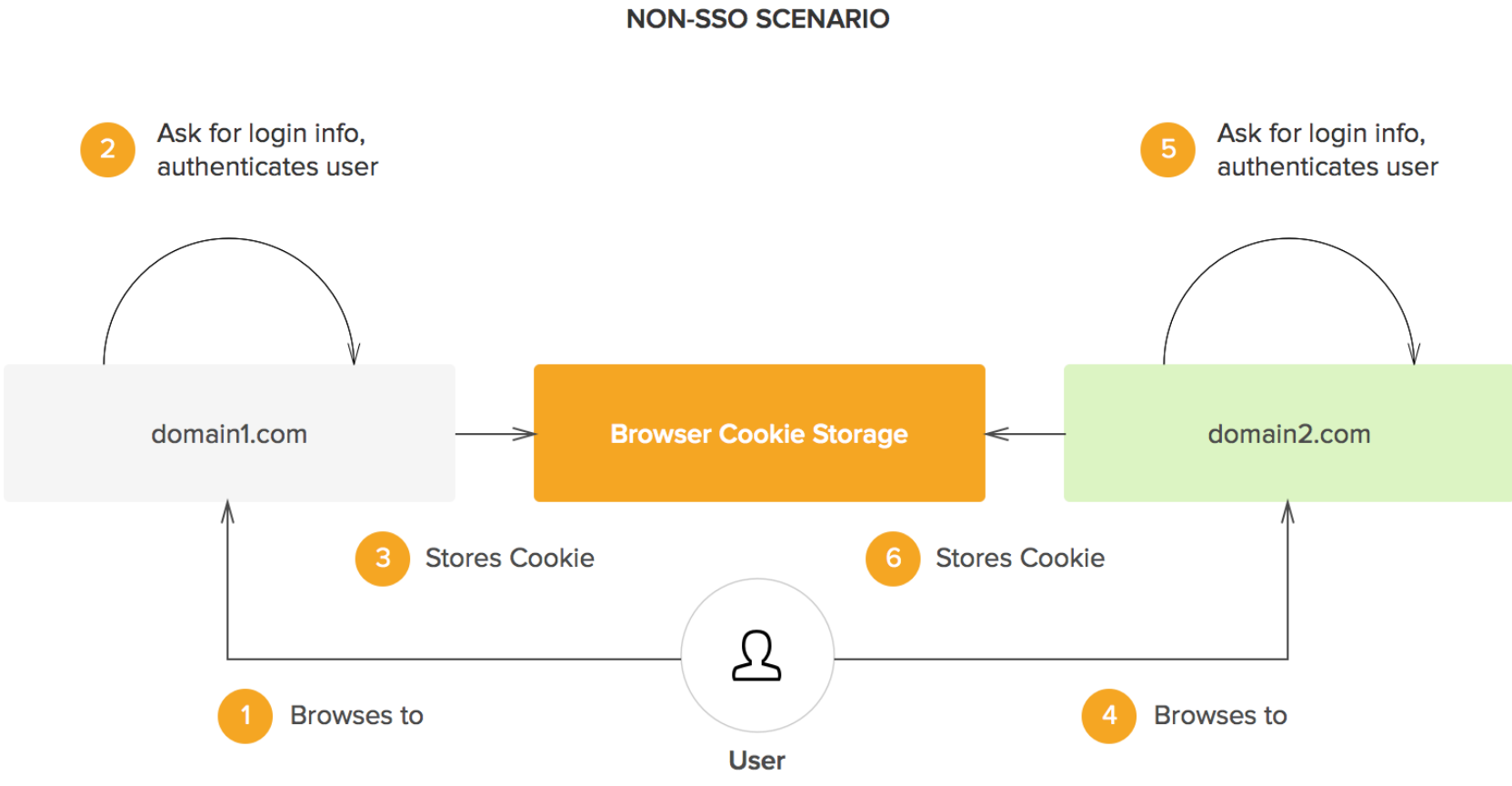
Об’єктом дослідження – є створення системи єдиного входу.

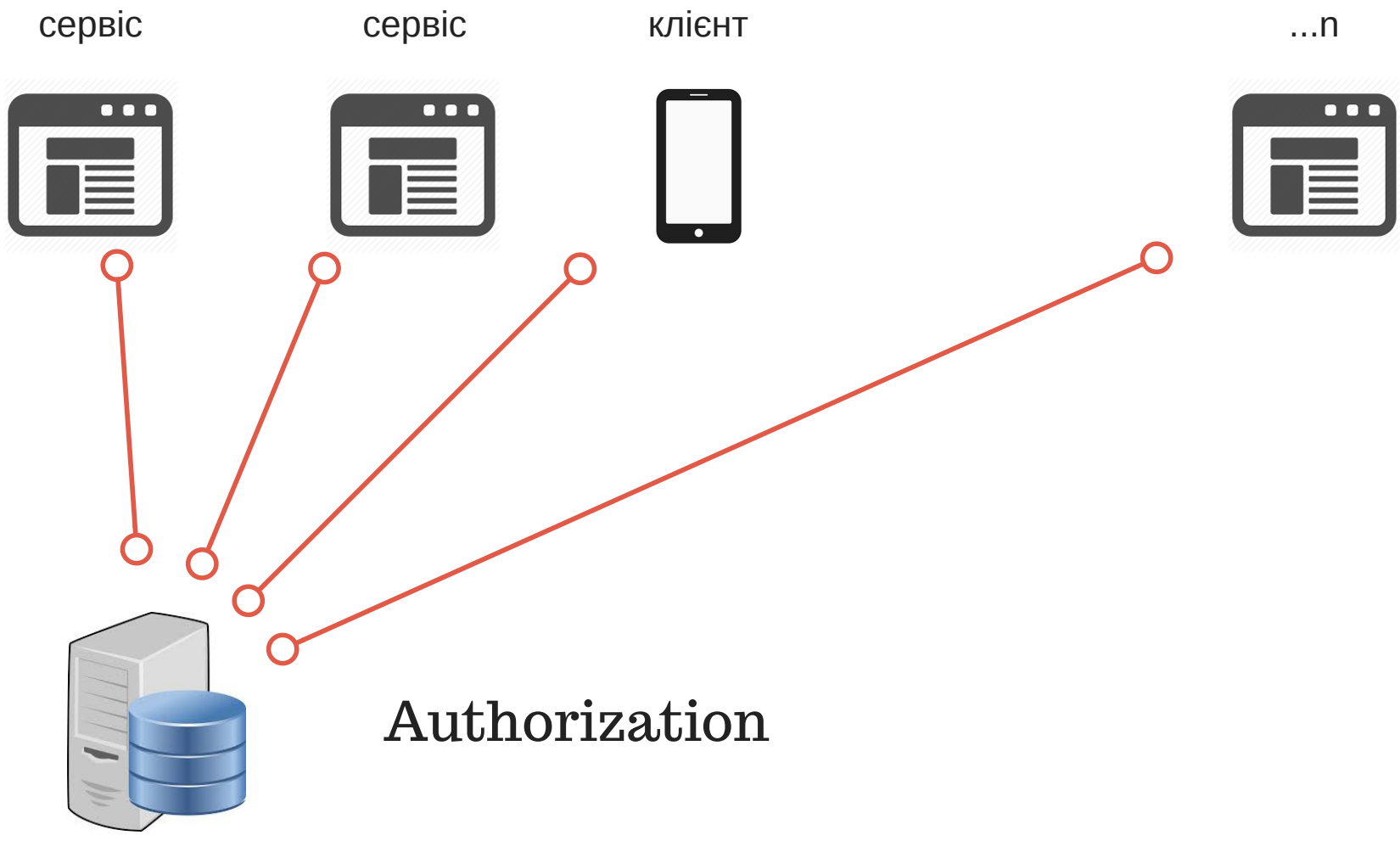
Предмет дослідження – є системи єдиного входу та протоколи авторизації у поєднанні із стандартними механіками аутентифікації користувачів.

Аутентифікація – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора.

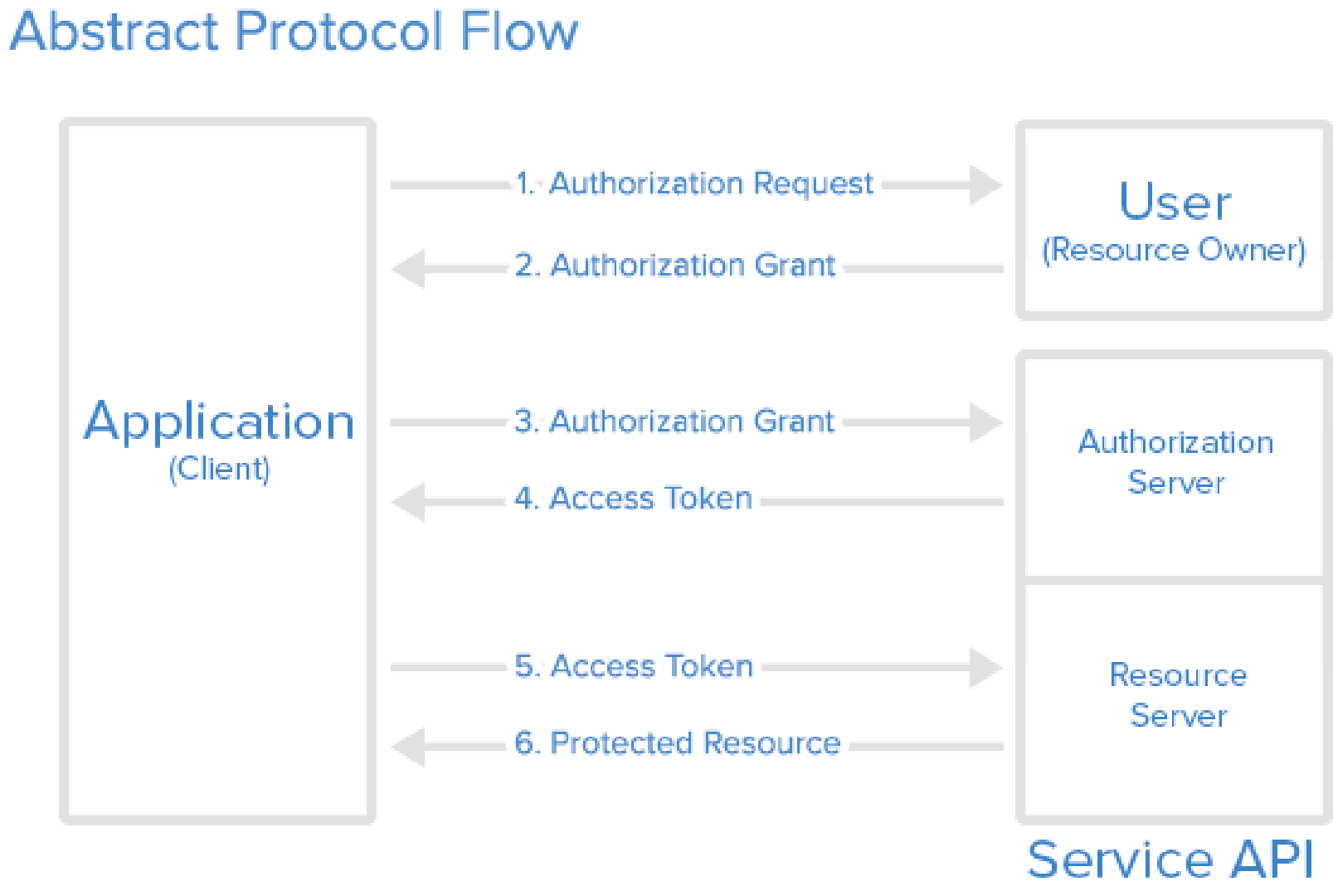
Авторизація – керування рівнями та засобами доступу до певного захищеного ресурсу, наприклад, автоматизована система контролю доступу та ресурсів системи залежно від ідентифікатора і пароля користувача або надання певних повноважень (особі, програмі) на виконання деяких дій у системі обробки даних.




NON-SSO SCENARIO
2
Ask for login info, authenticates user
5
Ask for login info, authenticates user
domain1.com
Browser Cookie Storage
domain2.com
3
Stores Cookie
6
Stores Cookie
1
Browses to
User
4
Browses to


сервіс
сервіс
клієнт
...n
Authorization

Oauth 2.0


Abstract Protocol Flow
Application
(Client)
1. Authorization Request
2. Authorization Grant
3. Authorization Grant
4. Access Token
5. Access Token
6. Protected Resource
User
(Resource Owner)
Authorization
Server
Resource
Server
Service API

Tokens flow

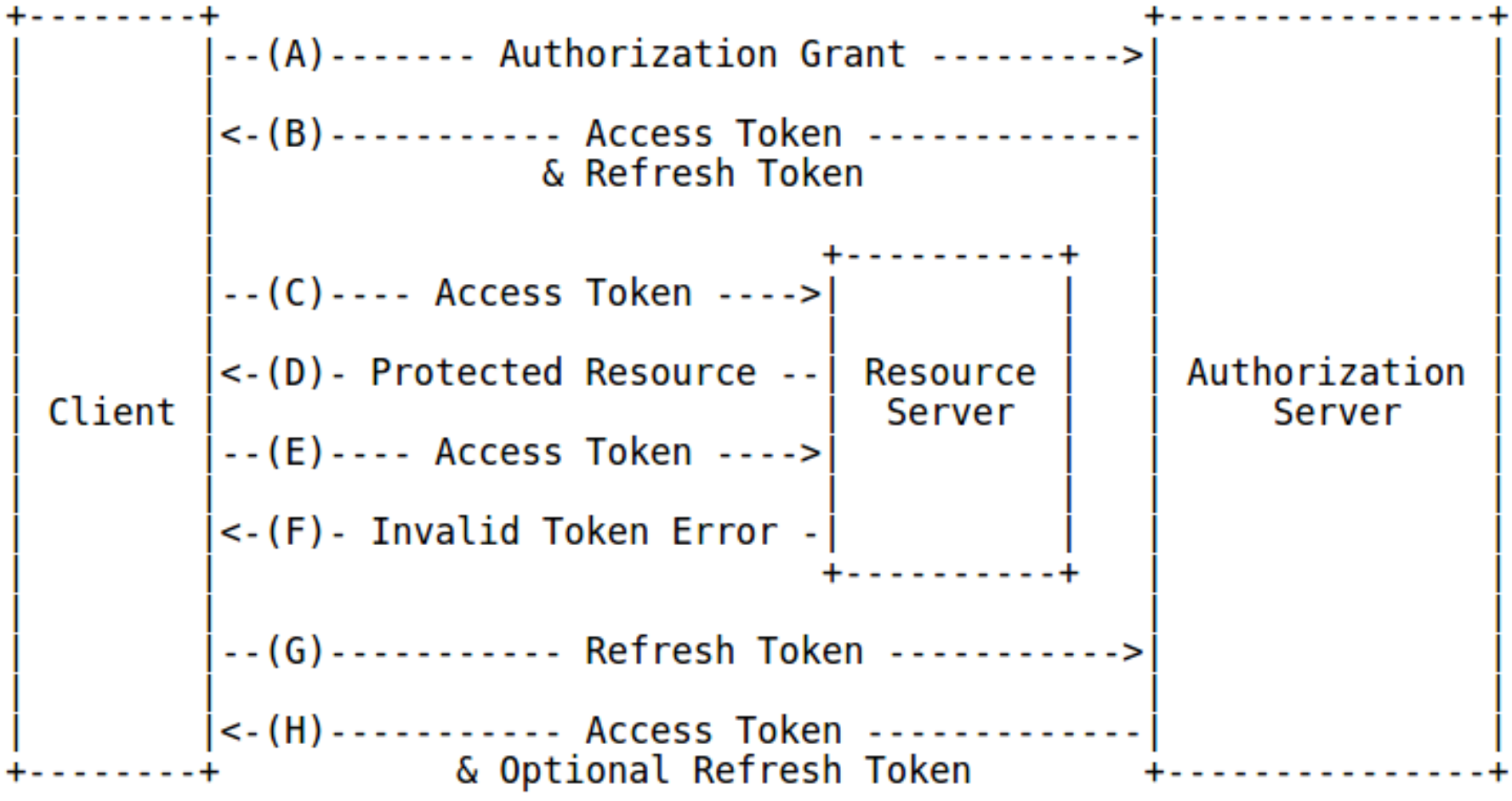


Figure 2: Refreshing an Expired Access Token

JWT

Encoded

```
eyJhbGciOiJIUzI1NiIsInR5c
CI6IkpXVCJ9.eyJzdWIiOiIxM
jM0NTY3ODkwIiwibmFtZSI6Ik
pvaG4gRG9lIiwiYWRtaW4iOnR
ydWV9.TJVA95OrM7E2cBab30R
MHrHDcEfxjoYZgeFONFh7HgQ
```

Decoded

```
{
  "alg": "HS256",
  "typ": "JWT"
}
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secret
)
```

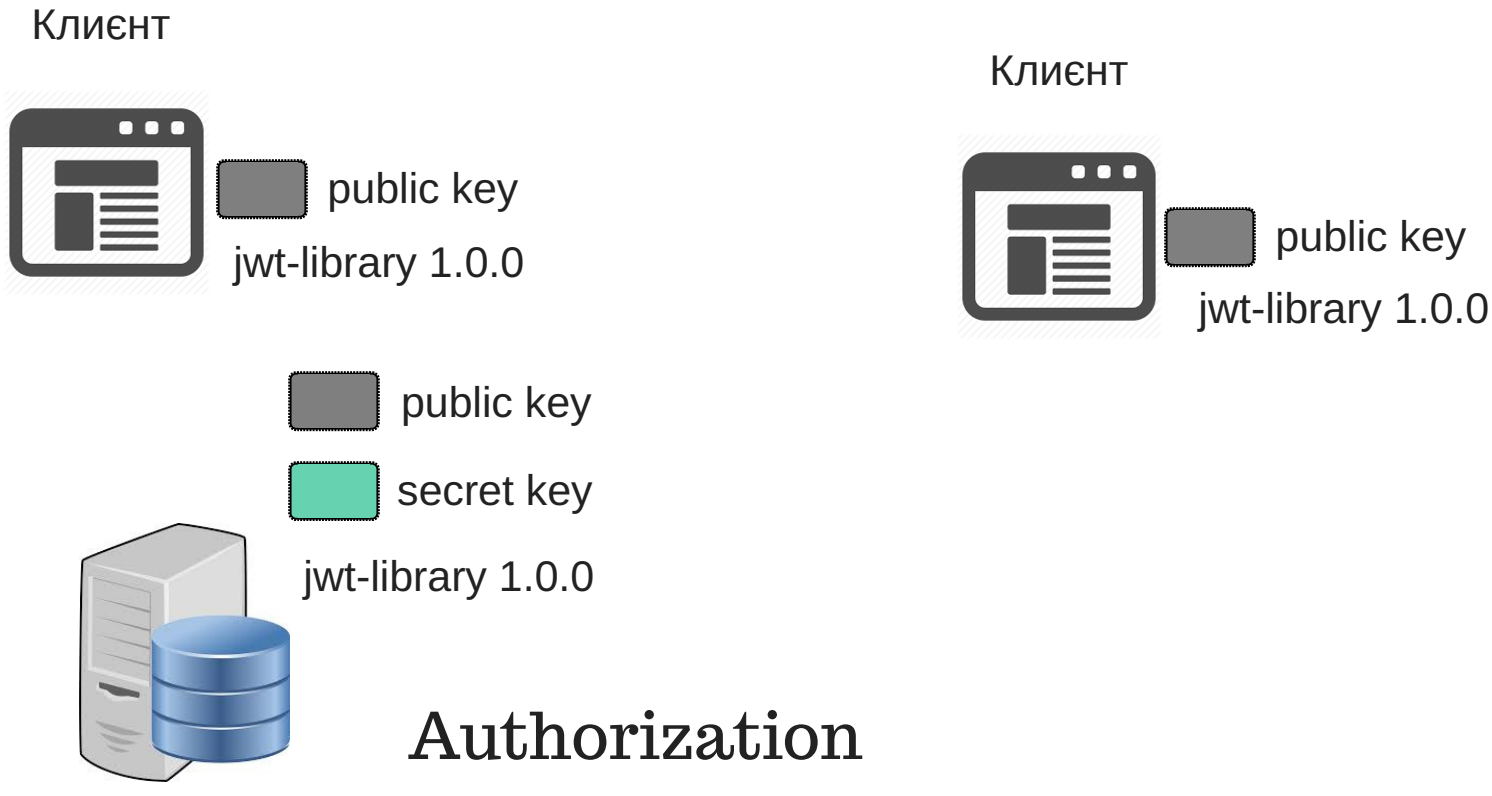
Header

Payload

Signature

"iss" (Issuer)
"sub" (Subject)
"aud" (Audience)
"exp" (Expiration Time)
"nbf" (Not Before)
"iat" (Issued At)
"jti" (JWT ID)

Взаємодія між клієнтами

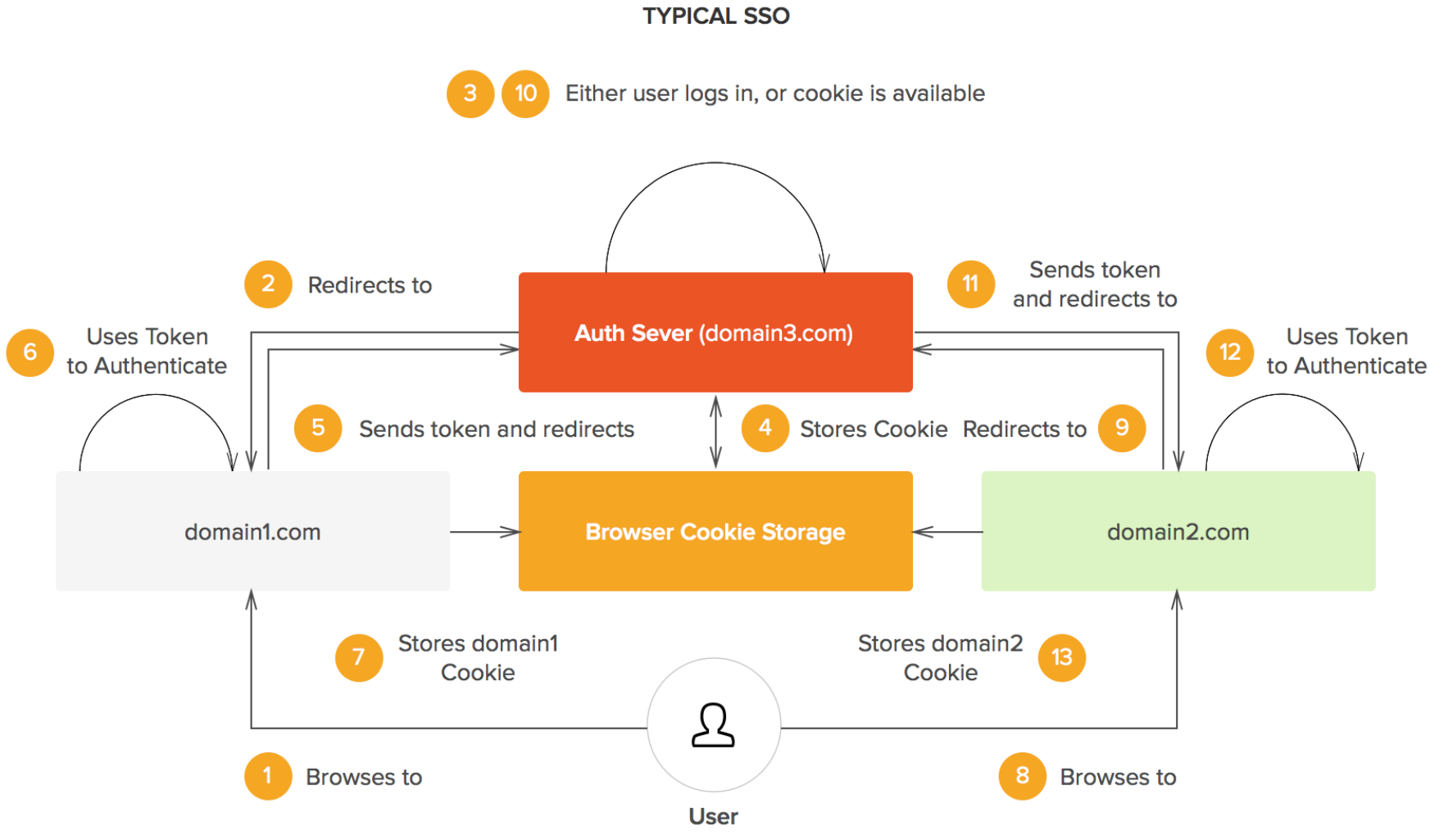


2.1. Client Types

OAuth defines two client types, based on their ability to authenticate securely with the authorization server (i.e., ability to maintain the confidentiality of their client credentials):

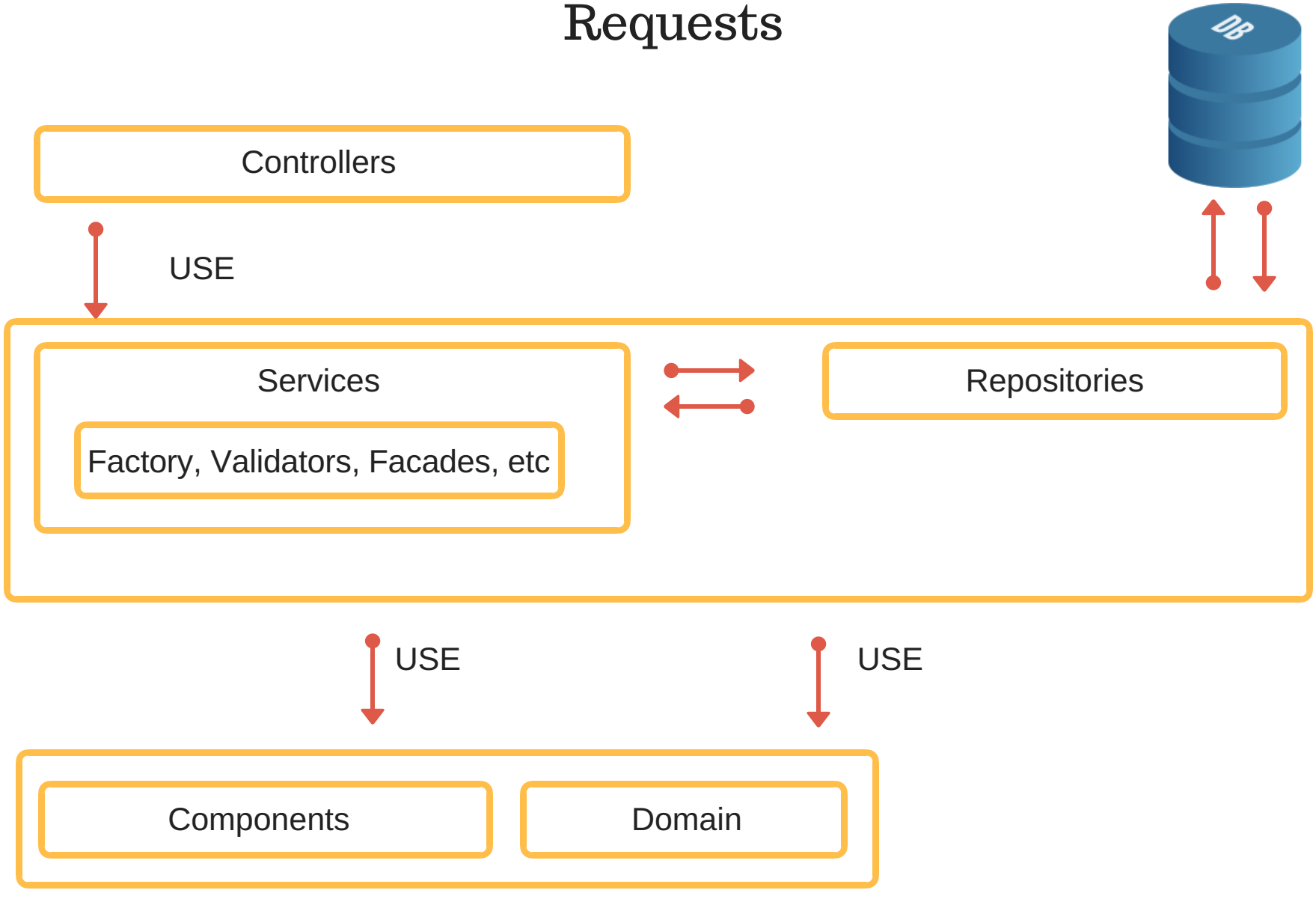
confidential
: Clients capable of maintaining the confidentiality of their credentials (e.g., client implemented on a secure server with restricted access to the client credentials), or capable of secure client authentication using other means.

public
: Clients incapable of maintaining the confidentiality of their credentials (e.g., clients executing on the device used by the resource owner, such as an installed native application or a web browser-based application), and incapable of secure client authentication via any other means.


TYPICAL SSO
3
10
Either user logs in, or cookie is available
2
Redirects to
Auth Sever (domain3.com)
11
Sends token
and redirects to
6
Uses Token
to Authenticate
12
Uses Token
to Authenticate
5
Sends token and redirects
4
Stores Cookie
Redirects to
9
domain1.com
Browser Cookie Storage
domain2.com
7
Stores domain1
Cookie
Stores domain2
Cookie
13
1
Browses to
8
Browses to
User

Предметно-орієнтоване проектування та **SOLID** принципи

Requests


DB
Controllers
USE
Services
Factory, Validators, Facades, etc
Repositories
USE
USE
Components
Domain

Висновки

Основними достоїнствами системи єдиного входу є:

Зниження кількості паролів, необхідних для різних програмних продуктів;

Зниження часу, необхідного для повторного введення паролів;

Зниження навантаження на мережу, пов'язаної з багаторазовими процедурами аутентифікації;

Зниженні вартості IT-системи за рахунок зниження кількості інцидентів ІБ, пов'язаних з обліковими даними користувачів;