DOI: 10.59647/978-617-520-936-3/1

Сучасні протоколи автентифікації та авторизації: аналіз OAuth 2.0, OIDC та SAML

Владислав Сусідко, здобувач ступеня вищої освіти магістр[1] (ORCID: 0009-0002-8652-8393), **Нікіта Панагода,** здобувач ступеня вищої освіти магістр[1](ORCID: 0009-0005-0174-900X), **Тамара Лященко,** ст. викладач кафедри ІТ[1] (ORCID: 0000-0001-9092-0297)

[1] *Київський національний університет будівництва і архітектури, 03037, м. Київ, проспект Повітряних Сил, 31, Україна*

АНОТАЦІЯ

В цій роботі проведено огляд і порівняння трьох ключових протоколів для автентифікації та авторизації в веб-додатках: OAuth 2.0, OpenID Connect (OIDC) та SAML (Security Assertion Markup Language). Проаналізовано особливості їхньої реалізації, архітектуру та випадки використання. Висвітлено переваги й недоліки кожного протоколу з точки зору безпеки, масштабованості та сумісності з сучасними системами. Це дослідження є важливим для розуміння вибору найкращого протоколу для конкретних застосувань.

Ключові слова: OAuth 2.0, OIDC, OpenID Connect, SAML, автентифікація, авторизація, безпека.

1. ВСТУП

Сучасні інформаційні системи вимагають надійних і безпечних методів автентифікації та авторизації для забезпечення захисту даних користувачів. Три основні технології, що широко використовуються для цих завдань — OAuth 2.0, OpenID Connect та SAML — стали стандартами у веб-технологіях і забезпечують різні рівні безпеки та зручності у використанні. У цій роботі ми проведемо порівняльний аналіз цих трьох протоколів для виявлення їхніх ключових особливостей і визначимо, яка технологія підходить для певних випадків використання.

2. МЕТА РОБОТИ

Мета цього дослідження — порівняти три основні протоколи автентифікації та авторизації: OAuth 2.0, OpenID Connect і SAML. У фокусі порівняння — безпека, функціональність та застосування кожного з цих рішень у контексті інтеграції в сучасні системи.

3. ДОСЛІДЖЕННЯ

Автентифікація та авторизація є основними складовими сучасних інформаційних систем, які забезпечують безпечний доступ до ресурсів. З розвитком інтернету та хмарних технологій з'явилася необхідність стандартизованих протоколів, які можуть безпечно передавати дані між різними системами. Основною задачею таких протоколів є забезпечення правильного ідентифікування користувача та надання доступу до відповідних ресурсів, виходячи з прав користувача.

З розвитком технологій безпеки з'явилися різні стандарти, що відповідають вимогам сучасного ринку. Три основні протоколи, що стали популярними, це OAuth 2.0, OpenID Connect та SAML. Кожен із цих протоколів має свої унікальні характеристики і підходить для різних сценаріїв використання. Далі буде розглянуто особливості та архітектура кожного з них.

3.1. OAuth 2.0

OAuth OAuth 2.0 — це фреймворк для авторизації, який широко використовується для забезпечення доступу сторонніх додатків до ресурсів користувача без необхідності надання облікових даних. Він функціонує на основі маркерів доступу (access tokens), які видаються клієнтським додаткам після проходження авторизації.

Основні компоненти OAuth 2.0 включають:

- ресурсний власник (Resource Owner) — користувач, чиї ресурси запитуються.
- клієнт (Client) — додаток, що запитує доступ до ресурсів користувача.
- сервер авторизації (Authorization Server) — сервіс, що надає маркери доступу після успішної авторизації.
- ресурсний сервер (Resource Server) — сервіс, що захищає ресурси і перевіряє валідність маркера.

OAuth 2.0 підтримує кілька сценаріїв авторизації, включаючи "Authorization Code", "Implicit", "Client Credentials" та "Password Grant". Основною перевагою цього протоколу є його гнучкість та можливість використання в різних сценаріях, таких як мобільні додатки, веб-сайти, API.

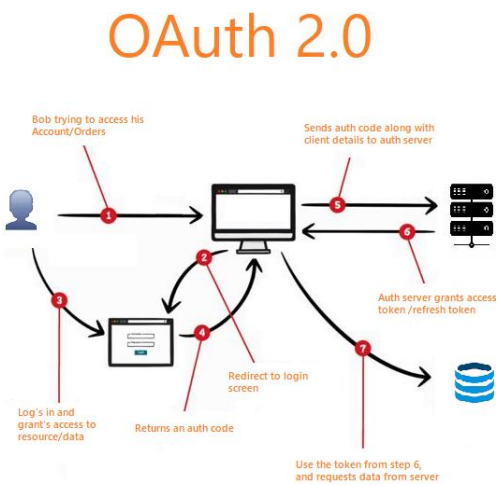

Рисунок 2. Схема роботи OIDC

3.2. OpenID Connect (OIDC)

OpenID OpenID Connect — це розширення OAuth 2.0, яке додає механізм автентифікації до наявного процесу авторизації. OIDC дозволяє клієнтському додатку отримати інформацію про користувача через спеціальний токен — "id token", що містить дані про особу користувача. Це робить OpenID Connect популярним рішенням для систем єдиної автентифікації (SSO).

Основні компоненти OIDC включають ті ж самі елементи, що і в OAuth 2.0, але додається ID-токен, який містить закодовану інформацію про автентифікованого користувача.

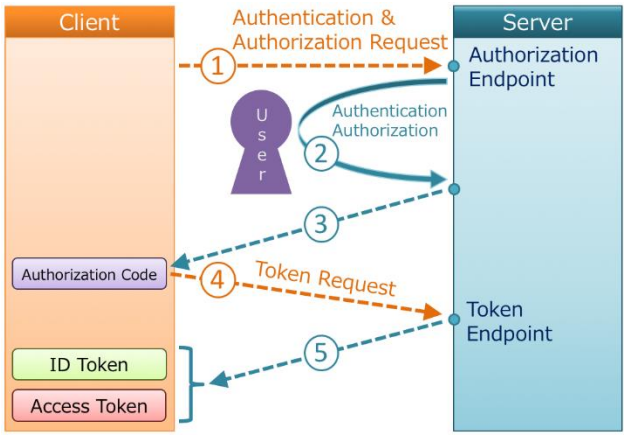

Рисунок 2. Схема роботи OIDC

3.3. SAML (Security Assertion Markup Language)

SAML — це XML-стандарт для обміну інформацією про автентифікацію та авторизацію між різними системами. Його основна функція полягає в тому, щоб забезпечити єдину автентифікацію (SSO) між декількома доменами. SAML зазвичай використовується у великих корпораціях для забезпечення взаємодії між різними внутрішніми системами, що потребують високого рівня захисту.

Основні компоненти SAML включають:

- постачальник ідентичності (Identity Provider) — сервіс, що здійснює автентифікацію користувача.
- постачальник послуг (Service Provider) — додаток або сервіс, який отримує інформацію про автентифікацію від Identity Provider.
- assertion — XML-документ, який містить інформацію про автентифікацію користувача та його права доступу.

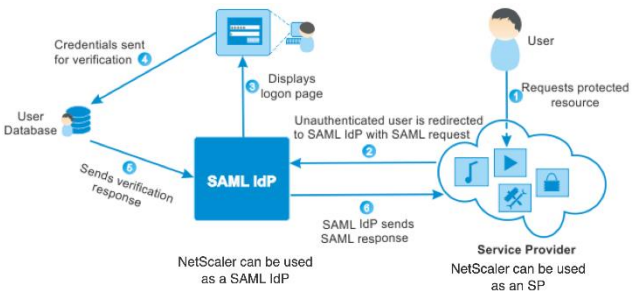

Рисунок 3. Схема роботи SAML

4. РЕЗУЛЬТАТ

Порівняння трьох протоколів показало, що кожен з них має свої унікальні переваги та недоліки. OAuth 2.0 забезпечує гнучку авторизацію, проте вимагає додаткових механізмів для автентифікації, що робить OpenID Connect зручним вибором для тих, кому потрібні обидві функції. SAML, зі свого боку, залишається найпопулярнішим рішенням для корпоративних систем, де є вимога до високого рівня безпеки та контролю доступу.

5. ВИСНОВКИ

Вибір між OAuth 2.0, OpenID Connect та SAML залежить від конкретних потреб системи. OAuth 2.0 є універсальним рішенням для авторизації, але вимагає розширення для автентифікації. OpenID Connect підходить для інтеграції з мобільними додатками та забезпечення простоти автентифікації. SAML, попри складність інтеграції, залишається потужним інструментом для корпоративних середовищ, де пріоритетом є безпека. Отже, важливо ретельно оцінювати вимоги до безпеки та зручності кожної системи перед впровадженням певного протоколу.

Список літератури

[1] Hardt D. The OAuth 2.0 Authorization Framework. IETF, 2012. 76 p. URL: https://doi.org/10.17487/rfc6749

[2] Sakimura N., Bradley J., Jones M. OpenID Connect Core 1.0. The OpenID Foundation, vol. 335, 2014. 91 p.

[3] Cantor S. Security Assertion Markup Language (SAML) V2.0 Technical Overview. OASIS, 2005. 54 p.

[4] Jones M., Bradley J., Sakimura N. OAuth 2.0 Authorization Framework: Bearer Token Usage. IETF, 2012. 22 p. URL: https://doi.org/10.17487/rfc6750

[5] Dhanjani N. OAuth 2.0 and the Road to Hell. IEEE Internet Computing, vol. 17, no. 6, 2013, pp. 58-63.

[6] Hughes J., Maler E., Mishra P. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS, 2005. 92 p.

[7] Naik N. Choice of OAuth 2.0/OpenID Connect for Developing Identity Management Solutions. IEEE, 2018. pp. 494-499.