

## **Рецензія на публікацію:**

### **«Корпоративне управління доступом на основі самоврядної цифрової ідентичності»**

#### **Введення**

У цій публікації досліджується потенціал парадигми «Self-Sovereign Identity (SSI)» для вдосконалення систем «Управління ідентифікацією та доступом (IAM)» у корпоративних середовищах. Автори ставлять два центральних дослідницьких питання:

- Які вимоги до IAM на підприємствах?
- Як SSI може допомогти задовольнити ці вимоги?

Основною метою дослідження є не тільки класифікація вимог до IAM, але й оцінка того, як SSI - децентралізована, криптографічно безпечна модель ідентифікації - може поліпшити існуючі IAM-рішення. Автори розробляють прототип IAM системи на базі SSI, демонструють її функціональність та оцінюють її ефективність за допомогою експертних інтерв'ю.

#### **Методологія**

Дослідження ґрунтується на методології «Design Science Research (DSR)», яка поєднує інженерний та поведінковий підходи для створення артефактів, що вирішують проблеми реального світу. ДСР складається з трьох фаз:

- Цикл актуальності - виявлення проблеми та вимоги до дослідження
- Цикл проектування - побудова та тестування прототипу
- Цикл строгості - підтвердження наукового внеску та узагальнення результатів

*Для збору даних автори провели:*

- "Систематичний огляд літератури (SLR)" - безліч статей, вибираючи деякі для глибокого аналізу
- "Кодування вимог" - авторами зроблено вибір кодової групи за категоріями
- «Напівструктуровані інтерв'ю» з експертами з подальшим тематичним кодуванням лоту

Ґрунтуючись на цьому аналізі, автори згрупували вимоги до ІАМ за чотирма всеосяжними категоріями:

- А) Безпека та відповідність вимогам
- Б) Працездатність
- В) Технології
- Г) Користувач

Прототип був побудований з використанням "Hyperledger Aries Cloud Agent (ACA - Py)" і "Hyperledger Indy", з цифровим гаманцем "Esatus AG". Він включає процеси видачі, використання та відкликання «перевірених облікових даних (VC)».

## Результатів

Дослідження демонструє, що прототип на основі SSI може відповідати вимогам усіх чотирьох категорій ІАМ:

1. Безпека та відповідність вимогам
  - ✓ Використання «доказів з нульовим розголошенням (ZKPs)»
  - ✓ Верифікація без розкриття повних облікових даних
  - ✓ Відкликання облікових даних через реєстр блокчейну
2. Працездатність
  - ✓ Автоматизація видачі та відкликання
  - ✓ Швидкий онбординг та офбординг
  - ✓ Зниження навантаження на ІТ-відділи
3. Технології
  - ✓ Сумісність з OIDC/OAuth
  - ✓ Підтримка поступової інтеграції
  - ✓ Використання стандартів (ВК, ВП, ДІД)

#### 4. Користувач

- ✓ Автентифікація без пароля
- ✓ Контроль користувачів за розкриттям даних
- ✓ Прозорість через інтерфейс цифрового гаманця

Експерти підтвердили, що SSI має потенціал для покращення систем IAM, особливо з точки зору безпеки, керованості та користувацького досвіду. Вони також відзначили такі проблеми, як технічна термінологія, залежність від підключення до мережі для перевірок відкликаних і відсутність ланцюжка облікових даних.

### Ключові висновки

#### *1. SSI забезпечує забезпечення найменших привілеїв через ZKP*

Це має вирішальне значення для безпеки підприємства. Це забезпечує точний контроль доступу без розкриття повних облікових даних. Це може стати основою для побудови гнучких моделей ABAC.

#### *2. Відкликання венчурного капіталу на основі блокчейну є надійним механізмом офбордингу*

Цей механізм дозволяє швидко деактивувати доступ при звільненні співробітників. Це, як практичний інструмент для автоматизації управління життєвим циклом доступу, особливо в середовищах з високою плинністю кадрів.

#### *3. SSI підтримує поступову інтеграцію з існуючими IAM-системами*

Можливість використовувати атрибути VP у веб-токенах JSON для OAuth створює міст між застарілими та сучасними системами. Це стратегічно важливо для міграції без ризику поточних інвестицій в інфраструктуру.

#### *4. Гаманці SSI забезпечують прозорість і контроль користувачів*

Користувачі можуть бачити, хто запросив їхні облікові дані, і відкликати доступ. Це життєво важливо для побудови довіри в системах, де конфіденційність має першорядне значення. На практиці це може покращити дотримання GDPR та розширити можливості користувачів.





## *5. Відсутність ланцюжка облікових даних є обмеженням масштабованості*

Це розуміння є важливим як виклик, який потрібно вирішити. У великих організаціях, де облікові дані мають бути пов'язані, ця функціональність має важливе значення. Це слід враховувати при оцінці готовності SSI до розгортання на підприємстві.

### **Висновок**

Дана робота робить значний внесок у дослідження «децентралізованих систем IAM». Авторами класифіковано вимоги корпоративного IAM та створено прототип, який демонструє практичну життєздатність SSI. Вони показують, що SSI може покращити безпеку, керованість, технологічну сумісність та користувацький досвід.

*Подальші дослідження можуть бути проведені за такими напрямками:*

-  Порівняльний аналіз SSI з традиційними платформами IAM (наприклад, Keycloak, Azure AD)
-  Інтеграція SSI з Zero Trust та IoT
-  Вплив безпарольної автентифікації на поведінку користувачів
-  Проектування ланцюжків облікових даних і масштабованих моделей відкликання

Якщо ви практикуєтеся в розробці архітектури безпеки, вам варто врахувати цю роботу в напрямку створення гнучких, прозорих і автоматизованих систем доступу, щоб створене середовище відповідало сучасним стандартам і потребам.

## **Словник**

### **Самосуверенна ідентичність (SSI)/(Дослівний переклад: Self-Sovereign Identity (SSI))**

Модель цифрової ідентифікації, за якої окремі особи або організації повністю володіють і контролюють свої ідентифікаційні дані, не покладаючись на централізовані органи влади. SSI дозволяє користувачам керувати обліковими даними та вибірково розкривати інформацію за допомогою криптографічних доказів.

### **Керування ідентифікаційними даними та доступом (IAM)/ Identity and Access Management (IAM)**

Структура політик і технологій для забезпечення належного доступу потрібних людей до технологічних ресурсів. Системи IAM керують цифровими ідентифікаціями, аутентифікацією, авторизацією та контролем доступу.

**Джерело:** NIST SP 800-53, ISO/IEC 27001

### **Наукові дослідження в галузі дизайну (DSR)/ Design Science Research (DSR)**

Методологія дослідження, яка зосереджена на створенні та оцінці артефактів, призначених для вирішення виявлених проблем. Він поєднує строгість (наукове обґрунтування) з актуальністю (практичною корисністю).

### **Систематичний огляд літератури (SLR)/ Systematic Literature Review (SLR)**

Структурований метод виявлення, оцінки та синтезу існуючих досліджень з певної теми. Він дотримується попередньо визначених протоколів для забезпечення прозорості та відтворюваності.

### **Кодування за вимогами/ Requirement Coding**

Техніка якісного аналізу даних, яка використовується для категоризації та інтерпретації текстових даних (наприклад, стенограми інтерв'ю, література) за значущими кодами та темами. Часто використовується в обґрунтованій теорії та тематичному аналізі.

## **SourSemi-структуровані інтерв'ю/ SourSemi-Structured Interviews**

Якісний метод дослідження, що передбачає керовані бесіди з відкритими питаннями. Це забезпечує гнучкість у вивченні тем, зберігаючи узгодженість між учасниками.

## **Хмарний агент Hyperledger Aries (ACA-Py)/ Hyperledger Aries Cloud Agent (ACA-Py)**

Агентський фреймворк на основі Python з відкритим вихідним кодом для створення додатків SSI. Він підтримує обмін повідомленнями DIDComm, обмін обліковими даними та інтеграцію з Hyperledger Indy.

## **Hyperledger Indy**

Розподілений реєстр, спеціально створений для децентралізованої ідентифікації. Він підтримує перевірені облікові дані, DID-адреси та механізми автентифікації зі збереженням конфіденційності.

## **Перевірені облікові дані (VC)/ Verifiable Credentials (VCs)**

Стандарт W3C для цифрових облікових даних, які мають криптографічний підпис і можуть бути перевірені без звернення до емітента. Венчурні капіталісти підтримують вибіркове розкриття та докази зі збереженням конфіденційності.

## **Доведення з нульовим розголошенням (ZKP)/ Zero-Knowledge Proofs (ZKPs)**

Криптографічні протоколи, які дозволяють одній стороні довести іншій, що твердження є правдивим, не розкриваючи жодної інформації, що виходить за межі дійсності твердження.

## **Відкликання облікових даних/ Credential Revocation**

Процес визнання недійсним раніше виданого посвідчення з метою запобігання його використанню в майбутньому. У SSI відкликання часто керується за допомогою криптографічних реєстрів на блокчейні.

## **Реєстр блокчейнів/ Blockchain Registry**

Децентралізована книга обліку, яка реєструє транзакції або зміни стану (наприклад, видачу облікових даних, відкликання) із захистом від несанкціонованого доступу. Використовується в SSI для зберігання відкритих ключів, схем і даних про відкликання.

## **OIDC (OpenID Connect)**

Рівень ідентичності, побудований на основі OAuth 2.0, який дозволяє клієнтам перевіряти особистість кінцевих користувачів на основі автентифікації, виконаної сервером авторизації.

## **OAuth 2.0**

Фреймворк авторизації, який дозволяє програмам отримувати обмежений доступ до облікових записів користувачів у службі HTTP без розкриття облікових даних користувача.

**Джерело:** IETF RFC 6749

## **VC (Verifiable Credential)**

Цифрова заява, видана суб'єктом (емітентом) про суб'єкта, криптографічно підписана та така, що підлягає перевірці. Він містить твердження та метадані.

**Джерело:** модель даних W3C Verifiable Credentials Model

## **VP (Презентація, що піддається перевірці)/ VP (Verifiable Presentation)**

Структура даних, яка містить один або кілька перевірених облікових даних, які власник надає верифікатору. Він підтримує вибіркове розкриття та підтвердження володіння.

**Джерело:** модель даних W3C Verifiable Credentials Model

## **DID (децентралізований ідентифікатор)/ DID (Decentralized Identifier)**

Глобальний унікальний ідентифікатор, який не потребує централізованого реєстраційного органу. DID вирішують документи DID, що містять публічні ключі та кінцеві точки обслуговування.

**Джерело:** W3C Специфікація децентралізованих ідентифікаторів (DID) v1.0

## **Прозорість через інтерфейс цифрового гаманця/ Transparency via Digital Wallet Interface**

Можливість для користувачів переглядати, керувати та контролювати свої облікові дані, з'єднання та розкриття інформації за допомогою безпечного та зручного інтерфейсу.

**Джерело:** Рекомендації щодо UX для гаманців SSI (наприклад, Lissi, Trinsic, esatus)

## **Веб-токени JSON для OAuth/ JSON Web Tokens for OAuth**

Компактний, безпечний за URL-адресою засіб представлення претензій, що підлягають передачі між двома сторонами. JWT використовуються в OAuth 2.0 як токени на пред'явника для контролю доступу.

**Джерело:** IETF RFC 7519; OAuth.net Довідник JWT

## **GDPR (Загальний регламент про захист даних)**

Регламент Європейського Союзу (EU 2016/679), який регулює обробку персональних даних і захищає права фізичних осіб на недоторканність приватного життя. Він вимагає прозорості, згоди, мінімізації даних та підзвітності.

**Джерело:** офіційний текст GDPR - EUR-Lex



## **Бенчмаркінг SSI з Zero Trust та IoT/ Benchmarking SSI with Zero Trust and IoT**

Новий напрям досліджень, який оцінює, як принципи SSI (ідентифікація, контрольована користувачем, вибіркове розкриття) можуть бути інтегровані з архітектурами Zero Trust та екосистемами IoT для підвищення безпеки, масштабованості та довіри на рівні пристрою.