Технічні вимоги

Щодо неприпустимості використання OpenID Connect токенів при наявності eIDAS/EUDI у вимогах

2026

Зміст

Зміст

Анотація

ТЕХНІЧНІ ВИМОГИ

1. Нормативно-правова база

Законодавство Європейського Союзу прямо вимагає використання архітектури Європейської цифрової ідентичності (EUDI) та регламенту eIDAS для електронної ідентифікації високого рівня assurance (High/Low/Substantial). Це виключає застосування стандартного протоколу OpenID Connect як самостійного або основного механізму автентифікації в системах, що підлягають інтеграції з європейськими стандартами цифрової ідентичності.

Ключові нормативні акти:

- Регламент (ЄС) № 910/2014 (eIDAS) та його оновлення (eIDAS 2.0) — обов'язкові вимоги до електронної ідентифікації та довірчих послуг, включаючи QTSP, mDOC та OpenID4VC.
- European Digital Identity Wallet Architecture and Reference Framework (ARF) — обов'язкова децентралізована модель EUDI Wallet з протоколами OpenID4VCI / OpenID4VP.
- ETSI TR 119 476 V1.2.1 (2024-07) — Electronic Signatures and Trust Infrastructures.

Стандартний OpenID Connect не відповідає вимогам децентралізації, вибіркового розкриття атрибутів та захисту конфіденційності, передбаченим EUDI.

2. Короткий зміст

Використання OpenID Connect як основного механізму цифрової ідентифікації в умовах обов'язкових вимог eIDAS та EUDI є технічно та нормативно невідповідним. EUDI базується на децентралізованій моделі з контролем доступу на основі атрибутів (ABAC), протоколами OpenID4VC, форматом mDOC та криптографічними доказами без CRL/OCSP. Стандартний OpenID Connect є централізованою моделлю з bearer-токенами і не забезпечує цих властивостей.

3. Рекомендації

У системах, що підлягають вимогам eIDAS та EUDI, пріоритетним є використання повної архітектури EUDI Wallet з протоколами OpenID4VC, mDOC та інтеграцією з кваліфікованими надавачами довірчих послуг (QTSP).

Стандартний OpenID Connect не рекомендується як самостійний механізм. Рекомендована схема:

- автентифікація та видача атрибутів через EUDI Wallet (Holder) з використанням OpenID4VCI / OpenID4VP;
- верифікація презентацій (VP) через Verifier з обов'язковим логуванням криптографічних доказів;
- інтеграція з PKIX лише через кваліфіковані сертифікати QTSP.

4. Практика

EUDI Wallet передбачає обов'язкову децентралізовану модель: Issuer → Holder → Verifier, формат mDOC, вибіркове розкриття атрибутів та криптографічні докази. Стандартний OpenID Connect не підтримує жодної з цих вимог і не забезпечує:

- уникнення витоку метаданих через CRL/OCSP;
- посередницьку роль Holder;
- відповідність вимогам ETSI та ARF щодо кваліфікованих електронних атестацій атрибутів (QEAA).

5. Адвокат

Основні причини відмови від OpenID Connect як заміни EUDI/eIDAS:

1. Централізація. OpenID Connect залежить від єдиного Identity Provider. EUDI — розподілена модель без єдиного центру.
2. Відсутність конфіденційності. Bearer-токени розкривають повний набір атрибутів. EUDI забезпечує вибіркове розкриття через Holder.
3. Несумісність з CRL/OCSP. OpenID не усуває ризики витоку активності користувача.
4. Регуляторна невідповідність. eIDAS та ARF вимагають OpenID4VC + mDOC + QTSP.

6. Сутності

- OpenID Connect — централізований протокол федеративної ідентифікації з bearer ID-токенами (JWT).
- EUDI — децентралізована архітектура цифрової ідентичності ЄС на базі OpenID4VC, mDOC та PKIX.
- eIDAS — регламент ЄС щодо електронної ідентифікації та довірчих послуг.
- OpenID4VC — розширення OpenID для verifiable credentials (обов'язковий транспорт в EUDI).
- mDOC — формат мобільних документів ISO/IEC 18013-5.
- Verifiable Credentials / Presentations — криптографічно підписані атрибути з вибірковим розкриттям.

Висновок

Використання OpenID Connect як самостійного механізму цифрової ідентифікації в системах, що відповідають вимогам eIDAS та EUDI, є неприйнятним. Обов'язковим є застосування повної децентралізованої архітектури EUDI Wallet з протоколами OpenID4VC, mDOC та QTSP. Це єдина схема, яка забезпечує нормативну відповідність, захист конфіденційності та можливість трансграничної взаємодії.

Література

[1] European Commission. European Digital Identity Wallet Architecture and Reference Framework.

[2] Regulation (EU) No 910/2014. Regulation on electronic identification and trust services (eIDAS).

[3] ETSI TR 119 476 V1.2.1 (2024-07). Electronic Signatures and Trust Infrastructures.

[4] OpenID for Verifiable Credential Issuance and Presentation.

[5] OWASP Foundation. OWASP Top 10: The Ten Most Critical Web Application Security Risks.

[6] NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations.

[7] IETF RFC 7519. JSON Web Token (JWT).

[8] WALT.ID — Open Source EUDI/OpenID4VC compatible solution.

[9] AUTHLETE.COM — EUDI compatible platform.