ЕЛЕКТРОННІ КОМУНІКАЦІЇ

DOI: 10.20535/kpisn.2024.1-4.315076
УДК 004.056

О.О. Стеценко
КПІ ім. Ігоря Сікорського, Київ, Україна
Відповідальний автор: stetsenko.alexander@lll.kpi.ua

АНАЛІЗ СЕРТИФІКАЦІЇ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ В УКРАЇНІ

Проблематика. Сертифікація електронних довірчих послуг в Україні стикається з кількома проблемами. Ці виклики включають необхідність узгодження з міжнародними стандартами, забезпечення стійкості криптографічної інфраструктури проти кіберзагроз, що посилюються, і узгодження практики з положенням Європейського Союзу про eIDAS. Крім того, проблеми, пов'язані з сумісністю, правовими межами та загальною безпекою електронних довірчих послуг, створюють значні перешкоди.
Мета дослідження. Сприяння зміцненню національної системи кібербезпеки України шляхом вирішення проблем, пов'язаних із сертифікацією електронних довірчих послуг, з акцентом на компоненти криптографії та процес сертифікації.
Методика реалізації. Передбачає багатоаспектний підхід. Вивчення наявних систем оцінки відповідності, глобального досвіду та регуляторних механізмів у провідних країнах з акцентом на ЄС. Оцінювання сильних і слабких сторін поточних електронних довірчих послуг в Україні. Порівняння нормативно-правової бази та технічних механізмів, що діють для електронних довірчих послуг в ЄС та Україні. Пропонування практичних рекомендацій для систем акредитації та оцінювання відповідності в Україні для приведення у відповідність з регламентом ЄС eIDAS.
Результати дослідження. Дослідження дає цінну інформацію про виклики, з якими стикаються українські електронні довірчі служби, особливо щодо оцінки наявної системи сертифікації. Порівняльний аналіз виявляє прогалини та можливості для вдосконалення, зосереджуючись на узгодженні практик з положенням ЄС про eIDAS. Емпіричні дані дають детальне розуміння точок зору та проблем ключових зацікавлених сторін. Дослідження також визначає конкретні сфери для вдосконалення правових і технічних аспектів електронних довірчих послуг.
Висновки. Є нагальна потреба в системному вдосконаленні сертифікації електронних довірчих послуг в Україні, зокрема у криптографічних центрах сертифікації ключів. Вирішення цих викликів вимагає скоординованих зусиль для узгодження практики з міжнародними стандартами, посилення заходів кібербезпеки та сприяння взаємодії, а також підкреслює важливість постійного моніторингу, адаптації до нових загроз та співпраці з міжнародними партнерами для забезпечення ефективності й безпеки електронних довірчих послуг в Україні.
Ключові слова: сертифікація; електронні довірчі послуги; центри сертифікації ключів; регулювання eIDAS; кібербезпека; оцінка відповідності.

Вступ

В епоху, коли домінують цифрові транзакції та зв'язок, надійність і безпека електронних довірчих послуг (Electronic trust services (ETS)) є найважливішими для стабільності національних систем кібербезпеки. Дослідження заглиблюється у складну сферу сертифікації ETS, з акцентом на компоненти криптографії та процес сертифікації ETS. Оскільки цифровий ландшафт розвивається, узгодження практики сертифікації з установленими міжнародними стандартами стає не лише стратегічним імперативом, але й необхідним кроком до зміцнення інфраструктури кібербезпеки країни.

Постанова Європейського Союзу про eIDAS (від англ. ***e**lectronic **ID**entification, **A**uthentication and trust **S**ervices*, що дослівно означає «електронна ідентифікація, автентифікація та довірчі послуги») [1] слугує орієнтиром для дослідження, надаючи структуру, яка наголошує не лише на ефективності сертифікації, але й на її міжнародній гармонізації. Черпаючи натхнення у глобальному ландшафті, в описува-

Пропозиція для цитування цієї статті: О.О. Стеценко, "Аналіз сертифікації електронних довірчих послуг в Україні", *Наукові вісті КПІ*, № 1–4, с. 7–17, 2024. doi: 10.20535/kpisn.2024.1-4.315076

Offer a citation for this article: O.O. Stetsenko, "Analysis of certification of electronic trust services in Ukraine", *KPI Science News*, no. 1–4, pp. 7–17, 2024. doi: 10.20535/kpisn.2024.1-4.315076

ному документі проводиться аналіз сертифікації електронних довірчих послуг (ETS) на міжнародному рівні, щоб визначити найкращі практики та тенденції сертифікації та гармонізації з міжнародними стандартами.

Аналіз предмету дослідження виходить далеко за межі України і передбачає проведення дослідження як українських, так і закордонних джерел, щоб ретельно вивчити наявну систему сертифікації в Україні, визнаючи її сильні сторони та визначаючи сфери, які дозріли для вдосконалення. Висвітлюючи проблеми та пропонуючи прагматичні рішення, дослідження має на меті зробити внесок у практичні ідеї для підвищення безпеки та ефективності електронних довірчих служб.

Коли орієнтуєшся на складність сертифікації ETS, мета стає досить зрозуміла: прокласти шлях для більш безпечного, стандартизованого та міжнародного процесу сертифікації в Україні. Це дослідження є критичним дослідженням конвергенції кібербезпеки та ETS, прокладаючи курс на стійке й перспективне цифрове майбутнє.

Електронні довірчі послуги: поняття та значення

Електронні довірчі послуги є важливим компонентом сучасного цифрового ландшафту, який сприяє безпечній онлайн-взаємодії та транзакціям. Розглянемо концепції та значення, пов'язані з ETS, висвітлюючи їх важливість та різні форми.

Електронні довірчі послуги, які часто називають е-довірчими послугами, охоплюють широкий спектр онлайн-сервісів і механізмів, які встановлюють і підтримують довіру та безпеку в електронних транзакціях і комунікаціях. Ці служби відіграють ключову роль у забезпеченні конфіденційності, цілісності та автентичності електронних даних і транзакцій. Деякі поширені приклади ETS включають цифрові підписи, електронні печатки, штампування часу, електронні служби зареєстрованої доставки та автентифікацію вебсайтів.

Електронні довірчі послуги складаються з таких ключових компонентів [2]:

1. Цифрові підписи – криптографічний метод, що забезпечує автентифікацію та перевірку цілісності вмісту електронних документів або повідомлень, використовуючи для перевірки унікальний приватний ключ і відповідний відкритий ключ.

2. Електронні печатки – подібні до цифрових підписів, але використовуються організаціями для підтвердження джерела та цілісності документів.

3. Послуги встановлення часових позначок – надають надійні позначки часу, які можна перевірити, для електронних документів або транзакцій, важливі для юридичних цілей і доказів.

4. Автентифікація вебсайту – забезпечує легітимність і безпеку вебсайтів, часто реалізовані через сертифікати Secure Sockets Layer (SSL).

Криптографічні компоненти у довірчих службах

У сфері ETS криптографічні компоненти утворюють основу безпеки, забезпечуючи конфіденційність, цілісність і автентичність електронних даних і транзакцій.

Шифрування [3], фундаментальна криптографічна техніка, захищає конфіденційну інформацію від несанкціонованого доступу під час передачі чи зберігання. Воно перетворює відкритий текст на зашифрований за допомогою криптографічних алгоритмів і ключів. Ключові аспекти шифрування довірчих служб включають:

· Симетричне шифрування: використовує один секретний ключ як для шифрування, так і для дешифрування. Ефективний, але вимагає безпечного розповсюдження ключів.

· Асиметричне шифрування: також називають криптографією з відкритим ключем, воно використовує пару ключів – відкритий ключ для шифрування і закритий ключ для дешифрування. Забезпечує безпечне спілкування без необхідності безпечного обміну ключами.

Цифрові підписи [4], вирішальні в довірчих службах, автентифікують і перевіряють цілісність електронних документів і повідомлень. Основні аспекти включають:

· Відкритий і закритий ключі: передбачають використання пар відкритих і закритих ключів. Закритий ключ створює підпис, а відповідний відкритий ключ перевіряє його.

· Невідмова: цифрові підписи забезпечують невідмову, не дозволяючи підписантам заперечувати свою участь у підписанні документа чи повідомлення.

Криптографічні алгоритми є фундаментальними для роботи довірчих служб. Вони визначають спосіб шифрування, дешифрування та цифрових підписів. До відомих криптографічних алгоритмів відносять:

AES (Advanced Encryption Standard) [5]: AES, який широко використовують для симетричного шифрування, забезпечує надійний захист і високу продуктивність.

RSA (абревіатура від прізвищ Rivest, Shamir та Adleman) [6]: популярний асиметричний алгоритм шифрування, відомий безпекою та значним поширенням.

Криптографія еліптичної кривої (ECC – від англ. Elliptic-curve cryptography) [7]: ECC забезпечує надійний захист із меншою довжиною ключа, що робить його ефективним у середовищах з обмеженими ресурсами.

Криптографічні хеш-функції [8] відіграють вирішальну роль у забезпеченні цілісності та автентичності даних. Ключові аспекти криптографічних хеш-функцій включають:

· Стійкість до зіткнень: хороша хеш-функція повинна зробити обчислювально неможливим пошук двох різних вхідних даних, які дають однакове хеш-значення.

· Детермінованість: однакові вхідні дані завжди повинні давати однакове хеш-значення.

· Ефективність: хеш-функції мають бути ефективними для обчислення.

У довірчих службах **центри сертифікації ключів** [9] (КСС – від англ. key certification centers) видають цифрові сертифікати, які пов'язують криптографічні ключі з об'єктами. Криптографічні підсистеми КСС включають такі елементи:

· Генерація пар ключів: КСС генерують пари ключів і керують ними, забезпечуючи безпечне зберігання та розподіл відкритих і закритих ключів.

· Видача сертифіката: КСС видають цифрові сертифікати, що містять відкритий ключ власника сертифіката, підписаний закритим ключем КСС.

· Відкликання сертифіката: КСС керують відкликанням сертифіката у разі компрометації або проблем із безпекою, щоб запобігти зловживанням.

Огляд та оцінювання наявної системи оцінки сертифікації електронних довірчих послуг, їх складових

Оцінювання ETS – це критично важливий процес, призначений для оцінювання і підтвердження безпеки, надійності та відповідності цих послуг встановленим стандартам і правилам.

Сертифікаційне оцінювання є основою довіри та безпеки в епоху цифрових технологій. Його головна мета – встановити й підтримувати довіру до електронних довірчих послуг та їх постачальників.

Сертифікацію електронних довірчих послуг зазвичай проводять уповноважені органи. Ці організації забезпечують компетентність і неупередженість через акредитацію, яка часто контролюється національними органами, і дотримання таких стандартів, як ISO/IEC 17065. Основні міркування включають незалежність від оцінюваних організацій, технічний досвід у таких сферах, як інформаційна безпека, криптографія та відповідні стандарти, регулятивний нагляд і визначені терміни дії сертифікатів, що потребує періодичної переоцінки для подальшої відповідності.

Оцінювання наявних систем сертифікації ETS є вирішальним кроком у розумінні їхніх сильних і слабких сторін, а також можливостей для вдосконалення.

Основою для ETS в Україні став Закон України «Про електронні довірчі послуги» [10], який було прийнято з метою приведення практики України у відповідність до нормативних актів Європейського Союзу, зокрема Регламенту eIDAS (Електронна ідентифікація та довірчі послуги). Ця законодавча база створила основу для регулювання та сертифікації ETS у країні.

Відповідно до статті 32 Закону України «Про електронні довірчі послуги» суб'єкти, у тому числі юридичні особи та фізичні особи-підприємці, які мають намір надавати електронні довірчі послуги, можуть добровільно пройти процедуру [11] оцінювання відповідності за власний кошт. Цей порядок, який регламентується Кабінетом Міністрів України, оцінює відповідність вимогам до кваліфікованих надавачів ETS. Акредитовані органи з оцінювання відповідності, суб'єкти, акредитовані національними органами з акредитації, проводять це оцінювання у сфері ETS. Оцінювання враховує законодавство щодо кваліфікованих електронних довірчих послуг, особливо для суб'єктів ринків фінансових послуг, що регулюються Національним банком України, та операторів/учасників платіжних систем, а також враховує законодавство про захист інформації.

Процедура оцінювання відповідності у сфері електронних довірчих послуг

У сфері ETS процедура оцінювання відповідності передбачає вибір клієнтом органу з оцінювання відповідності та укладення договору. Клієнт може обрати іноземний орган, акредито-

ваний міжнародними органами, такими як Міжнародний форум з акредитації або Європейське співробітництво з акредитації.

Оцінювання, яке проводять у два етапи, включає перевірку документації та виїзд на місце для підтвердження результатів і перевірених послуг аудитом. Після кожного етапу формуються звіти, а орган з оцінювання відповідності видає документ про відповідність на основі аналізу звіту про аудит. Оцінювання проводять відповідно до ДСТУ ETSI EN 319 403-1:2021 та ДСТУ ETSI TS 119 403-2:2021 з урахуванням потреб замовника щодо усунення виявлених недоліків. Орган з оцінювання відповідності звітує про всі висновки клієнта, деталізуючи їх значний вплив на безпеку і здатність надавати кваліфіковані ETS.

Під час процедури оцінювання відповідності, якщо замовник має намір продовжити процеси щодо забезпечення відповідності своїх ETS вимогам стандартів та нормативних актів, він повинен надати органу з оцінкиювання відповідності план усунення виявлених недоліків. Орган проводить оцінювання коригувальних заходів, оцінює терміни виконання та інформує замовника про додаткові завдання для підтвердження.

Коригувальні дії щодо незначних невідповідностей, які мають обмежений вплив на безпеку та здатність обслуговування, мають бути вжиті протягом трьох місяців або, якщо вони складні, протягом шести місяців після повідомлення.

Після проведення оцінювання орган з оцінювання відповідності приймає рішення про повну відповідність або невідповідність вимогам ETS. Результатом рішення щодо відповідності [12] є підписаний документ, який видається замовнику, тоді як рішення про невідповідність включає аудиторський звіт із детальними висновками та виявленими недоліками.

Кваліфіковані постачальники ETS, зазначені в Довірчому списку, проходять регулярне оцінювання відповідності кожні 24 місяці. Орган з оцінкиювання відповідності встановлює програму для періодичного оцінювання на місці для перевірки відповідності вимогам ETS. Позапланове оцінювання враховує обставини, викладені у ДСТУ ETSI EN 319 403-1:2021 та ДСТУ ETSI TS 119 403-2:2021.

Кваліфіковані виконавці зобов'язані оперативно інформувати Держспецзв'язку про проведення як планового, так і позапланового оцінювання, надавши протягом трьох робочих днів документи відповідності та аудиторські звіти.

Органи з оцінювання відповідності роблять результати оцінювання ETS загальнодоступними.

Довірчий список

Довірчий список, яким керує Центральний засвідчувальний центр [13], регулярно оновлюється та безпечно публікується на його офіційному вебсайті. Він містить відомості про кваліфікованих постачальників довірчих послуг та про зміст їхніх ETS. Цей список відповідає обов'язковим вимогам, встановленим Кабінетом Міністрів України (КМУ), і дотримується порядку ведення, затвердженого Міністерством цифрової трансформації.

Файл надає інформацію про кваліфікованих постачальників довірчих послуг та їхні послуги з використанням алгоритмів електронного підпису, визначених ETSI TS 119 312:2021 та ДСТУ 4145-2002. Крім того, містить деталі щодо надавачів та послуги відповідно до «Порядку проведення експериментального проекту щодо взаємного визнання електронних довірчих послуг між Україною та Європейським Союзом», затвердженого постановою КМУ від 22.10.2022 № 1311. Файл довірчого списку є загальнодоступним і містить електронну печатку для автоматизованої обробки.

Довірчі списки з переліком КНЕДП для використання ЕДП в межах України.

Довірчі списки в Україні документують кваліфікованих постачальників довірчих послуг (КПДП) для використання довірчих послуг у межах країни, розділених на три сегменти:

1. Транскордонний довірчий список [14].
2. Списки довіри для ДП в Україні [15].
3. Списки довіри для використання ДП в Україні (ДСТУ ETSI TS 119 312:2021) [16].ёёё

Електронний реєстр чинних, блокованих і скасованих сертифікатів відкритих ключів

На вебсайті [17] розміщено електронний реєстр (табл. 1), який містить відомості про дійсні, заблоковані та відкликані сертифікати відкритих ключів. Ця електронна база даних містить різноманітні сертифікати, наприклад сертифікати електронної печатки Центрального засвідчувального органу (ЦЗО), які використовуються в режимі реального часу. Він також містить сертифікати кваліфікованих постачальників ETS (надалі – постачальники), створені за допомогою сертифіката електронної печатки

***Таблиця* 1.** Кваліфіковані надавачі електронних довірчих послуг

№ з/п	Юридична особа	Кваліфікований надавач електронних довірчих послуг
1	АКЦІОНЕРНЕ ТОВАРИСТВО КОМЕРЦІЙНИЙ БАНК «ПРИВАТБАНК»	Кваліфікований надавач електронних довірчих послуг АЦСК АТ КБ «ПРИВАТБАНК»
2	Військова частина 2428	Кваліфікований надавач електронних довірчих послуг «Військова частина 2428» Державної прикордонної служби України
3	Генеральний штаб Збройних сил України	Кваліфікований надавач електронних довірчих послуг «Центр сертифікації ключів Збройних сил України»
4	Офіс Генерального прокурора	Кваліфікований надавач електронних довірчих послуг органів прокуратури України
5	Державна казначейська служба України	Кваліфікований надавач електронних довірчих послуг Державної казначейської служби України
6	Акціонерне товариство «Оператор ринку»	Кваліфікований надавач електронних довірчих послуг «АЦСК ринку електричної енергії»
7	Державне підприємство «ДІЯ»	Кваліфікований надавач електронних довірчих послуг «ДІЯ»
8	...	...

Центрального органа сертифікації (ЦОС) із власним підписом. Реєстр вказує статус, обмеження використання та списки відкликаних сертифікатів, виданих ЦОС.

Міністерство цифрової трансформації України наказом від 28 липня 2020 року (№ 112) [18] затвердило Порядок ведення цього реєстру. Кваліфіковані провайдери, зазначені в Довірчому списку, можуть пропонувати виключно електронні довірчі послуги в банківській системі України та під час переказу коштів.

Як центральний сертифікуючий орган Міністерство забезпечує включення довірчого списку інформації про кваліфікованих постачальників та їхні послуги у форматі, придатному для автоматизованої обробки.

Глобальна система сертифікації електронних довірчих послуг: Європа

Європа, й особливо Європейський Союз, є піонером у розробленні комплексної та стандартизованої системи сертифікації ETS. Регламент eIDAS (Електронна ідентифікація та довірчі послуги), запроваджений у 2016 р., є наріжним каменем цієї прогресивної структури.

Регламент eIDAS є основним інструментом, що формує ландшафт сертифікації в Європі. Він встановлює узгоджену структуру для ETS, спрямовану на створення безперебійного і безпечного цифрового середовища у країнах-членах ЄС. Регламент охоплює різні компоненти, важливі для сертифікації ETS, від електронних підписів до постачальників довірчих послуг, встановлюючи узгоджений підхід для підвищення довіри до онлайн-взаємодії.

Основними цілями eIDAS є підвищення безпеки, надійності та транскордонної сумісності електронних транзакцій у межах ЄС. Він спрямований на створення правової основи, яка забезпечує надійність і юридичну дійсність електронних підписів і довірчих послуг, тим самим сприяючи єдиному цифровому ринку.

Одним із фундаментальних аспектів eIDAS є надання правового визнання електронних підписів та інших довірчих послуг. Регламент встановлює умови, за яких електронні підписи мають такий самий правовий статус, як і власноручні підписи, забезпечуючи юридичну визначеність для фізичних осіб і компаній, які беруть участь у цифрових транзакціях.

Згідно з цим регламентом держави-члени зобов'язані створювати, підтримувати і публікувати ***довірені списки***. Ці списки містять інформацію про кваліфікованих постачальників довірчих послуг і послуги, які вони пропонують. Довірені списки відіграють вирішальну роль у забезпеченні визначеності серед операторів ринку та сприянні сумісності кваліфікованих довірчих послуг.

Регламент eIDAS забезпечує правову основу для транскордонної електронної ідентифікації, автентифікації та сертифікації вебсайтів у межах ЄС. Він спрямований на створення передбачуваного нормативного середовища для електронних транзакцій у ЄС.

Довірчі списки ЄС

Держави-члени зобов'язані створювати, зберігати та публікувати довірені списки кваліфікованих надавачів довірчих послуг і послуг, які вони надають.

Відповідно до Регламенту про електронну ідентифікацію та довірчі послуги [19] для електронних транзакцій на внутрішньому ринку (Регламент eIDAS), національні довірчі списки мають установчу силу. Інакше кажучи, надавач довірчих послуг і довірчі послуги, які він надає, будуть кваліфіковані тільки в тому випадку, якщо він з'явиться у списку довірених осіб. Користувачі, включаючи громадян, підприємства та державні адміністрації, отримають юридичну силу, пов'язану з певною кваліфікованою довірчою послугою, лише якщо остання вказана як кваліфікована у списках довіри.

Стаття 22 Регламенту eIDAS зобов'язує держави-члени створювати, підтримувати і публікувати довірені списки. Ці переліки повинні включати інформацію, пов'язану з кваліфікованими надавачами довірчих послуг, за яких вони відповідають, та інформацію, пов'язану з кваліфікованими довірчими послугами, що надаються ними. Списки публікуються захищеним способом, з електронним підписом або печаткою у форматі, придатному для автоматизованої обробки.

Довірчі списки мають важливе значення для забезпечення визначеності між операторами ринку, оскільки вони вказують на статус постачальника послуг та послуги на момент нагляду. Вони спрямовані на сприяння інтероперабельності кваліфікованих довірчих послуг шляхом полегшення перевірки електронних підписів та електронних печаток тощо.

Держави-члени можуть додавати довірчі послуги, відмінні від кваліфікованих, до довірчих списків, на добровільній основі. Однак це лише на національному рівні, і слід чітко вказати, що вони не кваліфіковані відповідно до Регламенту eIDAS.

Для того, щоб надати доступ до довірених списків усіх держав-членів, Комісія через захищений канал до автентифікованого вебсервера надає громадськості довірені списки, нотифіковані державами-членами, у підписаній або скріпленій печаткою формі, придатній для автоматизованої обробки.

Правова база та гарантії в регулюванні eIDAS

Регламент eIDAS створює міцну правову основу для ETS, забезпечуючи безпечне та юридично визнане середовище. Він визначає умови дійсності та можливості виконання ETS, забезпечуючи прозорість цифрових транзакцій. Ця структура надає юридичну вагу документам із цифровим підписом, запечатаній інформації та даним із міткою часу, еквівалентним традиційним паперовим копіям, сприяючи юридичній визначеності та полегшуючи електронні транзакції.

Основні аспекти правової бази eIDAS включають:

- Невідмовність: Регламент гарантує, що автор електронного повідомлення чи транзакції не може заперечити участь, сприяючи підзвітності та довірі до цифрових взаємодій.
- Відповідність міжнародним стандартам: узгоджена з міжнародними стандартами структура eIDAS дозволяє державам-членам ЄС брати участь у безпечних цифрових транзакціях у всьому світі, сприяючи міжнародній співпраці та гармонізуючи правові стандарти.
- Обов'язки: визначено чіткі зобов'язання та відповідальність для постачальників довірчих послуг, кваліфікованих постачальників довірчих послуг і кінцевих користувачів, що створює прозоре та підзвітне середовище для електронних транзакцій.
- Захист кінцевих користувачів: Регламент містить гарантії захисту кінцевих користувачів від шахрайства, несанкціонованого доступу та інших ризиків, пов'язаних із цифровою взаємодією, встановлюючи баланс між перевагами ETS і захистом користувачів.
- Адаптивна структура: визнаючи динамічну природу технологій і правових ландшафтів, правова база eIDAS розроблена для постійного перегляду та адаптації. Регулярні оновлення забезпечують реагування на нові виклики, технологічний прогрес і зміни в законодавчих вимогах, зберігаючи надійність і актуальність фреймворку протягом тривалого часу.

Підсумовуючи, Глобальна система сертифікації ETS у Європі, прикладом якої є Регламент eIDAS, є комплексною і перспективною ініціативою. Звертаючи увагу на технологічні, правові та безпекові аспекти, ця система не тільки покращує національну систему кібербезпеки держав-членів ЄС, але й встановлює еталон для світових передових практик ETS. Прагнення до гармонізації, сумісності та адаптивності позиціонує ЄС як лідера у створенні безпечного та юридично визнаного середовища для електронних транзакцій. Порівняльний аналіз систем ETS України та ЄС показано у табл. 2

Таблиця 2. Порівняння системи сертифікації електронних довірчих послуг: Україна та Європейський Союз

Аспект системи сертифікації	Україна	Європейський Союз
Нормативно-правова база	Україна розробила нормативно-правову базу для ETS відповідно до міжнародних стандартів	ЄС має всеосяжну нормативно-правову базу, яка регулюється насамперед Регламентом eIDAS, що забезпечує юридичну ясність і правозастосовну силу
Оцінювання відповідності	Україна розробила свою систему оцінювання відповідності для ETS. Вона відбувається згідно із законом України «Про електронні довірчі послуги», стаття 32. «Оцінка відповідності у сфері електронних довірчих послуг»	ЄС, відповідно до Регламенту eIDAS, має добре налагоджену систему оцінювання відповідності, що забезпечує дотримання визначених стандартів
Криптографічні підсистеми	Україна розробляє та сертифікує криптографічні підсистеми для забезпечення безпеки ETS	ЄС через систему eIDAS здійснює сувору сертифікацію криптографічних підсистем, що охоплює алгоритми шифрування, управління ключами та інфраструктуру
Правове визнання	Україна визнає ETS відповідно до міжнародних стандартів. Згідно із Законом України «Про електронні документи та електронний документообіг», стаття 8	Регламент ЄС eIDAS забезпечує правове визнання, визначаючи умови, за яких ETS вважаються дійсними та примусово виконуваними
Транскордонне визнання	Україна прагне посилити транскордонне визнання своїх ETS відповідно до міжнародних стандартів	Регламент ЄС eIDAS сприяє транскордонному визнанню, дозволяючи безперешкодно здійснювати електронні транзакції між країнами-членами
Найважливіші стандарти та настанови	Україна приймає міжнародні стандарти та настанови щодо ETS як частину свого процесу сертифікації	ЄС покладається на стандарти, встановлені eIDAS, і дотримується міжнародних стандартів інтероперабельності та сумісності
Постійний моніторинг та адаптація	Кваліфіковані надавачі ETS кожні 24 місяці проходять процедуру оцінювання відповідності для доведення того, що вони та ETS, які ними надаються, відповідають вимогам	ЄС згідно з eIDAS включає положення про постійний моніторинг, забезпечуючи адаптацію системи сертифікації до нових викликів

Проблеми і рекомендовані рішення для вдосконалення електронних довірчих служб

Електронні довірчі послуги утворюють основу безпечних цифрових транзакцій, забезпечуючи основу для надійної взаємодії у цифровій сфері. Однак, щоб підтримувати свою ефективність і надійність, ці служби повинні орієнтуватися й подолати кілька проблем. Заглиблюючись у багатогранний ландшафт ETS, досліджуючи спільні виклики, з якими стикаються як в Україні, так і в усьому світі, від загроз кібербезпеці до юридичних складнощів, перешкоди, з якими стикаються ці служби, вимагають комплексних рішень, які поєднують технологічні інновації, нормативні вдосконалення та навчання користувачів.

Проблеми, які виникають у сфері ETS, не поодинокі; вони резонують у міжнародному масштабі. Оскільки цифрові транзакції стають все більш невід'ємною частиною нашого повсякденного життя, потреба у безпечній і надійній системі є першорядною. Таким чином, обговорення в цьому розділі зосереджено навколо конвергенції проблем і потенційних рішень, які можна застосовувати універсально. Незалежно від того, в Україні чи за кордоном, спільність цих викликів підкреслює спільну відповідальність за зміцнення ETS у всьому світі.

Для ефективного вирішення цих універсальних проблем важливо систематизувати їх та визначити перевірені рішення, які були успішно впроваджені в різних країнах. Аналізуючи повторювані виклики та усталені підходи до їх пом'якшення, надамо короткий список проблем і найбільш поширених рішень для подолання визначених проблем:

1. *Загрози кібербезпеці* [20].

1.1. *Проблеми*. Загрози кібербезпеці становлять серйозну проблему для електронних довірчих служб. Ці загрози можуть проявлятися в різ-

них формах, включаючи хакерство, зловмисне програмне забезпечення та інші зловмисні дії, що ставлять під загрозу цілісність і конфіденційність приватної інформації.

1.2. *Рішення*:

· Постійний моніторинг: впровадження надійних систем моніторингу для виявлення кіберзагроз та реагування на них у реальному часі.

· Розширені методи шифрування: використання найсучасніших методів шифрування для захисту даних від несанкціонованого доступу.

· Співпраця: налагодження спільних зусиль з експертами та організаціями з кібербезпеки, щоб бути у курсі нових загроз.

2. *Проблеми сумісності.*

2.1. *Проблеми*. Несумісність між різними системами та технологіями може перешкоджати безперебійній роботі електронних довірчих служб, що призводить до неефективності та потенційної вразливості.

2.2. *Рішення*:

· Стандарти сумісності: дотримання міжнародних стандартів сумісності для забезпечення сумісності різних систем.

· Інтеграція API: впровадження рішень інтерфейсу прикладного програмування (API) для полегшення зв'язку та обміну даними між системами.

· Регулярне тестування: проведення тестів на сумісність та оновлення для вирішення проблем і забезпечення безперебійної роботи.

3. *Правова та нормативна складність.*

3.1. *Проблеми*. Складне правове та нормативне середовище може створювати перешкоди для електронних довірчих служб, впливаючи на їх впровадження та ефективність.

3.2. *Рішення:*

· Гармонізація з міжнародними стандартами: узгодження національних нормативних актів із загальноприйнятими міжнародними стандартами, такими як положення ЄС про eIDAS.

· Чіткі вказівки щодо відповідності: надання чітких і лаконічних вказівок щодо відповідності, щоб зменшити двозначність і полегшити дотримання.

· Регулярні регулятивні оновлення: забезпечення регулярного оновлення нормативно-правової бази для вирішення нових технологічних проблем і викликів безпеки.

4. *Ризик шахрайства та викрадення особистих даних* [21].

4.1. *Проблеми*. Ризик шахрайства та крадіжки особистих даних становить загрозу для надійності електронних транзакцій і послуг.

4.2. *Рішення*:

· Багатофакторна автентифікація: реалізація багатофакторної автентифікації для додавання рівнів безпеки та перевірки особи користувача.

· Біометрична перевірка: включення біометричних методів автентифікації, таких як відбитки пальців або розпізнавання обличчя, для покращення перевірки особи.

· Системи виявлення шахрайства: використання передових систем виявлення шахрайства, які можуть ідентифікувати підозрілі дії та транзакції.

5. *Технологічний прогрес і старіння* [22].

5.1. *Проблеми*. Швидкі темпи технологічного прогресу можуть спричинити застаріваня наявних систем, потенційно призводячи до вразливості.

5.2. *Рішення:*

· Регулярні оновлення системи: забезпечення регулярного оновлення систем електронних довірчих служб для включення останніх виправлень безпеки та функцій.

· Напрями впровадження технологій: розроблення напряму впровадження нових технологій, щоб випереджати потенційні загрози.

· Інвестиції в R&D (від англ. – research and development): виділення ресурсів для досліджень і розробок, щоб передбачити майбутні технологічні виклики та вирішити їх.

6. *Транскордонне юридичне визнання* [1].

6.1. *Проблеми*. Відсутність транскордонного юридичного визнання може перешкоджати ефективності ETS у все більш глобалізованому цифровому середовищі.

6.2. *Рішення:*

· Міжнародна співпраця: співпраця з іншими країнами для укладення угод про взаємне визнання ETS.

· Гармонізація законодавчих меж: узгодження правових меж між кордонами для полегшення бездоганного визнання та прийняття електронних транзакцій.

· Участь у міжнародних ініціативах: активна участь у міжнародних ініціативах, спрямованих на створення стандартизованої правової бази для ETS.

Вирішення цих проблем вимагає спільних зусиль між державними установами, регуляторними органами, зацікавленими сторонами галузі та широким співтовариством для створення стійкого і надійного середовища для ETS. Рекомендовані рішення підкреслюють важливість багатогранного підходу, що включає технології,

регулювання, освіту та міжнародну співпрацю. Постійні дослідження, інформаційні кампанії та прогрес у технології й регулюванні є невід'ємною частиною подолання цих проблем і забезпечення постійного зростання ETS. Впроваджуючи ці заходи, зацікавлені сторони можуть сприяти постійному вдосконаленню та стійкості ETS, зміцненню довіри між користувачами та полегшенню безпечних цифрових транзакцій.

Вектори вдосконалення і майбутні технології в електронних довірчих службах

Оскільки ландшафт електронних довірчих служб розвивається, декілька векторів удосконалення та нових технологій готові підвищити ефективність, безпеку і досвід користувачів цих послуг. Ці вектори удосконалення представляють не лише негайні рішення, але й відомі загальні шляхи для розвитку безпечних цифрових послуг. Основні сфери вдосконалення та майбутні технології включають таке:

1. ***Технологія блокчейн*** **[23].**

Технологія блокчейн постає як трансформаційна сила у вдосконаленні ETS. Його децентралізована та незмінна природа забезпечує безпрецедентну прозорість, знижуючи ризик маніпулювання даними та несанкціонованого доступу. Використовуючи блокчейн, електронні довірчі служби можуть створювати стійкі до втручання контрольні стежки, забезпечуючи цілісність цифрових транзакцій.

2. ***Штучний інтелект*** (AI – від англ. Artificial Intelligence) і машинне навчання (ML – від англ. Machine Learning)**[24].**

Інтеграція AI та ML вводить динамічний рівень інтелекту в електронні довірчі служби. Ці технології дозволяють системам аналізувати величезні масиви даних, виявляти закономірності та вдосконалювати процеси прийняття рішень. AI та ML можуть значно покращити виявлення загроз, автентифікацію користувачів і загальну ефективність електронних довірчих служб.

3. ***Квантово-безпечна криптографія*** **[25].**

Оскільки поява квантових обчислень створює потенційну загрозу для криптографічних методів, впровадження квантово захищеної криптографії стає обов'язковим. Квантово стійкі алгоритми забезпечують постійну конфіденційність і цілісність ETS в умовах розвитку обчислювальних можливостей.

4. ***Біометрична автентифікація*** **[26].**

Біометрична автентифікація додає додатковий рівень безпеки електронним довірчим службам, покладаючись на унікальні фізіологічні чи поведінкові особливості. Цей персоналізований метод ідентифікації покращує процеси перевірки користувачів і знижує ризик неавторизованого доступу.

5. ***Безпека Інтернету речей*** (IoT – від англ Internet of Things) **[27].**

Із поширенням пристроїв IoT безпека взаємопов'язаної мережі стає першорядною для електронних довірчих служб. Посилення засобів захисту Інтернету речей від потенційних уразливостей, які можуть бути використані для порушення цілісності електронних транзакцій.

Враховуючи ці вектори вдосконалення та майбутні технології, ETS можуть не лише вирішувати поточні виклики, але й активно захищатися від нових загроз, забезпечуючи надійну та безпечну цифрову екосистему.

Висновки

1. Дослідження сертифікації ETS в Україні забезпечує глибоке розуміння поточних викликів і висвітлює критичні сфери для вдосконалення.

2. Аналізуючи українські процедури оцінювання відповідності та порівнюючи їх із визнаними міжнародними стандартами, особливо з регламентом ЄС eIDAS, дослідження підкреслює необхідність гармонізації з глобальними межами.

3. Основні рекомендації включають прийняття інтегрованих рішень для вирішення проблем кібербезпеки, проблем сумісності, регуляторних складнощів і технологічних досягнень, таких як блокчейн, штучний інтелект, квантово захищена криптографія, біометрична автентифікація та безпека Інтернету речей.

4. Це дослідження пропонує напрями для узгодження українських електронних довірчих служб з міжнародними стандартами та використання нових технологій для підвищення безпеки та ефективності як на національному, так і на глобальному рівнях.

References

[1] eIDAS Regulation website, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

[2] What are Electronic Trust Services?, https://edicomgroup.com/blog/what-are-electronic-trust-services.

[3] Difference Between Symmetric and Asymmetric Key Encryption, https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/.
[4] Digital signature, https://en.wikipedia.org/wiki/Digital_signature.
[5] Advanced Encryption Standard (AES), https://www.geeksforgeeks.org/advanced-encryption-standard-aes/.
[6] RSA Algorithm in Cryptography, https://www.geeksforgeeks.org/rsa-algorithm-cryptography/.
[7] Elliptic-curve cryptography, https://en.wikipedia.org/wiki/Elliptic-curve_cryptography.
[8] Cryptographic hash function, https://en.wikipedia.org/wiki/Cryptographic_hash_function.
[9] Certificate authority, https://en.wikipedia.org/wiki/Certificate_authority.
[10] Zakon Ukrainy Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy vid 01. 12. 2022, no. 2801, https://zakon.rada.gov.ua/laws/show/2155-19#Text.
[11] Postanova KM vid 13. 09. 2024, no. 1062, Pro zatverdzhennia Poriadku provedennia protsedury otsinky vidpovidnosti u sferakh elektronnoi identyfikatsii ta elektronnykh dovirchykh posluh, https://zakon.rada.gov.ua/laws/show/799-2023-п#n39.
[12] Zakon Ukrainy Pro zatverdzhennia vymoh u sferi elektronnykh dovirchykh posluh ta Poriadku perevirky dotrymannia vymoh zakonodavstva u sferi elektronnykh dovirchykh posluh vid 07. 11. 2018, no. 992, https://zakon.rada.gov.ua/laws/show/992-2018-п#n13.
[13] Elektronnyi reiestr diisnykh, pryzupynenykh abo vidklykanykh serytyfikativ vidkrytykh kliuchiv (czo.gov.ua), https://czo.gov.ua/en/ca-registry-details?type=0&id=131.
[14] Dovirchyi spysok z perelikom KNEDP dlia vykorystannia EDP transkordonno (czo.gov.ua), https://czo.gov.ua/trustedlist/3.
[15] Dovirchi spysky z perelikom KNEDP dlia vykorystannia EDP v mezhakh Ukrainy (czo.gov.ua), https://czo.gov.ua/trustedlist/2.
[16] Dovirchi spysky z perelikom KNEDP dlia vykorystannia EDP v mezhakh Ukrainy (czo.gov.ua), https://czo.gov.ua/trustedlist/1.
[17] Elektronnyi reiestr chynnykh, blokovanykh ta skasovanykh serytyfikativ vidkrytykh kliuchiv (czo.gov.ua), https://czo.gov.ua/ca_registry.
[18] Zakon Ukrainy Pro zatverdzhennia Poriadku vedennia reiestru chynnykh, blokovanykh ta skasovanykh serytyfikativ vidkrytykh kliuchiv vid 29. 07. 2020, no. 112, https://zakon.rada.gov.ua/laws/show/z0798-20#Text.
[19] Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repeali ng Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.
[20] 10 Emerging Cybersecurity Threats and Hacker Tactics in 2023, https://www.crn.com/news/security/10-emerging-cybersecurity-threats-and-hacker-tactics-in-2023?page=1.
[21] How to Tell the Difference Between Identity Fraud and Identity Theft?, https://www.mcafee.com/blogs/privacy-identity-protection/whats-the-difference-between-identity-fraud-and-identity-theft/.
[22] Global Risks Report 2022, Chapter 3. Digital Dependencies and Cyber Vulnerabilities. 2022, https://www.weforum.org/publications/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities/.
[23] What is blockchain?, https://www.ibm.com/topics/blockchain.
[24] Machine Learning vs. AI: Differences, Uses, and Benefits, https://www.coursera.org/articles/machine-learning-vs-ai.
[25] NIST Announces First Four Quantum-Resistant Cryptographic Algorithms, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.
[26] What is Biometric Authentication? A Complete Overview, https://heimdalsecurity.com/blog/biometric-authentication/.
[27] Internet of Things (IOT) security, https://www.imperva.com/learn/application-security/iot-internet-of-things-security/.

O.O. Stetsenko

ANALYSIS OF CERTIFICATION OF ELECTRONIC TRUST SERVICES IN UKRAINE

Background. Certification of electronic trust services in Ukraine faces several problems. These challenges include the need to align with international standards, ensure cryptographic infrastructure is resilient against evolving cyber threats, and align practices with the European Union's eIDAS regulation. In addition, issues related to interoperability, legal frameworks and the overall security of electronic trust services pose significant obstacles.

Objective. Contributing to the strengthening of the national cybersecurity system of Ukraine by solving problems related to the certification of electronic trust services, with an emphasis on cryptographic components and the certification process.

Methods. It involves a multifaceted approach. Study of existing conformity assessment systems, global experience and regulatory mechanisms in leading countries with an emphasis on the EU. Assessment of strengths and weaknesses of current electronic trust services in Ukraine. Comparison of the regulatory framework and technical mechanisms operating for electronic trust services in the EU and Ukraine. Offering practical recommendations for accreditation and conformity assessment systems in Ukraine to bring them into line with the EU eIDAS regulation.

Results. The study provides valuable information about the challenges faced by Ukrainian electronic trust services, especially regarding the assessment of the existing certification system. The benchmarking identifies gaps and opportunities for improvement, focusing on aligning practices with the EU eIDAS regulation. Empirical data provide a detailed understanding of the perspectives and

concerns of key stakeholders. The study also identifies specific areas for improvement in the legal and technical aspects of electronic trust services.

Conclusions. There is an urgent need for systematic improvement of the certification of electronic trust services in Ukraine, in particular in cryptographic key certification centers. Addressing these challenges requires a coordinated effort to align practices with international standards, strengthen cybersecurity measures, and promote interoperability. And also emphasizes the importance of constant monitoring, adaptation to new threats and cooperation with international partners to ensure the efficiency and security of electronic trust services in Ukraine.

Keywords: certification; electronic trust services; key certification centers; eIDAS regulation; cyber security; compliance assessment.

Рекомендована Радою
НН інституту телекомунікаційних систем
КПІ ім. Ігоря Сікорського

Надійшла до редакції
22 грудня 2023 року

Прийнята до публікації
4 квітня 2024 року