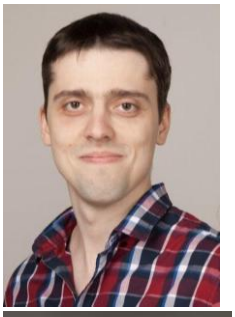
© Okhrimenko A., Stokipnyi O., Kovtun V. Analysis of the mobile-first model of qualified electronic signatures. // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 44-50. © This is an open access article under the CC BY 4.0 International license.*

DOI: 10.18372/2225-5036.32.21657

АНАЛІЗ МОДЕЛІ MOBILE-FIRST КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ПІДПИСІВ

Андрій Охріменко[1], Олександр Стокіпний[2], Влад Ковтун[3]

[1] Маріупольський державний університет
[2] Національний університет «Київський авіаційний інститут»
[3] Національний технічний університет «Харківський політехнічний інститут»



ОХРІМЕНКО Андрій Олександрович, к.т.н.
Дата та місце народження: 1990, м. Васильків, Київська обл., Україна
Освіта: Національний авіаційний університет, 2012
Посада: старший викладач кафедри системного аналізу та інформаційних технологій, Маріупольський державний університет
Наукові інтереси: криптографія, інфраструктура відкритих ключів, оптимізація криптографічних перетворень, безпека інформаційних систем
Основні роботи: понад 60 наукових праць, статті в фахових та міжнародних виданнях, патенти на корисну модель, авторські свідоцтва.
E-mail: a.okhrimenko@mu.edu.ua
ORCID: 0000-0001-8270-2863



СТОКІПНИЙ Олександр Леонідович, к.т.н.
Дата та місце народження: 1979, м. Гадяч, Полтавська обл., Україна
Освіта: Харківський військовий університет, 2002
Посада: доцент кафедри інтелектуальних кібернетичних систем, Національний університет «Київський авіаційний інститут»
Наукові інтереси: криптографія, ефективна реалізація криптографічних алгоритмів, розробка високонавантажених систем, архітектури сучасних програмних систем.
Основні роботи: понад 20 наукових праць, статті в фахових та міжнародних виданнях, авторські свідоцтва.
E-mail: oleksandr.stokipnyi@kai.edu.ua
ORCID: 0009-0007-4346-9684



КОВТУН Владислав Юрійович, к.т.н.
Дата та місце народження: 1978, смт. Петрове, Кіровоградська обл., Україна
Освіта: Харківський військовий університет, 2000
Посада: доцент кафедри програмної інженерії та інтелектуальних технологій управління, Національний технічний університет «Харківський політехнічний інститут»
Наукові інтереси: криптографія, алгебраїчні криві, ефективна реалізація криптографічних перетворень, прикладна математика, аналіз та алгебра
Основні роботи: понад 60 наукових праць, статті в фахових та міжнародних виданнях, патенти на корисну модель, авторські свідоцтва.
E-mail: vladislav.kovtun@gmail.com
ORCID: 0000-0002-4303-3510

Анотація. *У статті проведено комплексний аналіз моделі mobile-first кваліфікованих електронних підписів (КЕП) у контексті сучасних електронних довірчих послуг. Досліджено регуляторні засади функціонування remote QSCD відповідно до вимог eIDAS та eIDAS 2, а також процес гармонізації українського законодавства з європейською нормативною базою. Проаналізовано технічну архітектуру mobile-first підписання, включаючи механізми SCAL2, Signature Activation Data (SAD), Signature Activation Module (SAM), Hardware Security Module (HSM), Trusted Execution Environment (TEE) та Secure Enclave. Розглянуто основні моделі реалізації mobile-first КЕП, серед яких push-модель, QR-модель, федеративні схеми та інтеграція з EUDI Wallet. Проведено систематизацію загроз, спрямованих на мобільний застосунок, захищене середовище виконання, серверну інфраструктуру та канали зв'язку. Визначено перспективні напрямки розвитку mobile-first архітектур, зокрема інтеграцію постквантової криптографії, threshold cryptography, zero-knowledge proof та технологій розподіленого реєстру.*
Ключові слова: *кваліфікований електронний підпис, mobile-first, remote QSCD, eIDAS, електронні довірчі послуги, Signature Activation Module, Hardware Security Module, постквантова криптографія, EUDI Wallet.*

Вступ

Модель mobile-first кваліфікованого електронного підпису (КЕП) станом на 2025 рік стала домінуючим способом надання кваліфікованих довірчих послуг як у державах-членах Європейського Союзу (ЄС), так і в Україні. За даними Європейської Комісії та національних довірчих списків (Trusted Lists) більшість країн ЄС мають у своїх переліках кваліфікованих надавачів послуги віддаленого

© Okhrimenko A., Stokipnyi O., Kovtun V. Analysis of the mobile-first model of qualified electronic signatures. // Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 44-50. © This is an open access article under the CC BY 4.0 International license.

підписання [20], що технологічно реалізовані переважно через нативні мобільні застосунки. В Україні за результатами 2025 року сервіс «Дія.Підпис» обслуговує 8,7 мільйона унікальних підписувачів і випускає 31 мільйон кваліфікованих сертифікатів електронних підписів на рік (більшість з них саме через мобільний застосунок) [19], фактично виконуючи функцію національної мобільної схеми електронної ідентифікації. Основна ідея моделі mobile-first КЕП полягає в тому, що первинним інтерфейсом, через який громадянин користується довірчими послугами, є мобільний пристрій (переважно смартфон), при цьому особистий ключ громадянина зберігається на стороні кваліфікованого надавача електронних довірчих послуг (КНЕДП) у вигляді віддалено керованого кваліфікованого засобу створення підпису.

Попри своє широке застосування, модель mobile-first КЕП залишається сферою активних наукових, інженерних та регуляторних досліджень. Розвиток постквантової криптографії, поява нових послуг згідно eIDAS 2 та Європейського гаманця цифрової ідентичності EUDI Wallet, а також посилення регуляторних вимог, створюють серйозні виклики для моделі mobile-first.

Мета дослідження

Метою дослідження є проведення аналізу моделі mobile-first КЕП у регуляторній, технічній та науковій сфері, а також виявлення перспективних напрямків наукових та інженерних досліджень.

Регуляторна сфера mobile-first

До недавнього часу модель користування електронним підписом передбачала використання захищеного апаратного носія для зберігання особистих ключів підписувача. Даний захищений апаратний носій (переважно смарт-карта, чи USB-токен з інтегрованим криптографічним модулем) виступає захищеним чи кваліфікованим засобом створення підписів (Secure Signature Creation Device (SSCD) чи Qualified Signature and Seal Creation Device (QSCD)), що функціонує переважно в десктопному середовищі (дуже мало таких засобів, які інтегруються із мобільними пристроями), та дає виключну гарантію контролю підписувача над своїм особистим ключем. Проте така модель має недоліки, пов'язані з вартістю захищених носіїв, складнощами в їх експлуатації та неможливість їх швидкого використання поза робочим місцем. Зростання частки мобільних пристроїв у структурі цифрової взаємодії громадян, бізнесу та держави актуалізувало питання про правомірність зберігання кваліфікованого ключа підписувача не на персональному захищеному апаратному носії, а на стороні КНЕДП за умови забезпечення технічних та організаційних механізмів, які гарантують такий самий рівень виключного контролю підписувача над процесом створення підпису. Відповіддю на цей запит стало впровадження в нормативні документи віддаленого або серверного кваліфікованого засобу створення підпису (remote QSCD).

Прийняття Регламенту ЄС №910/2014 (eIDAS) вперше дозволило використовувати засіб створення кваліфікованого електронного підпису для управління особистим ключем підписувача за умов виконання ряду вимог [1]. Імплементаційне рішення Комісії ЄС 2016/650 встановило стандарти [4], на основі яких такі засоби сертифікуються (наприклад, CEN EN 419 241-1, CEN EN 419 241-2 та CEN EN 419 241-5). Саме це створило юридичні передумови для появи mobile-first архітектур, у яких підписувач взаємодіє з мобільним застосунком, а криптографічна операція виконується на Hardware Security Module (HSM) кваліфікованого надавача у центрі обробки даних.

Регламент ЄС 2024/1183 (eIDAS 2), ухвалений 11 квітня 2024 року, який модифікує Регламент № 910/2014, кваліфікує віддалене керування кваліфікованим засобом створення підпису (remote QSCD management, rQSCD) як самостійну кваліфіковану електронну довірчу послугу [2]. Надавачі, що пропонують дистанційне підписання, мають проходити кваліфікаційну оцінку безпосередньо за послугу управління засобом створення підпису, а не лише за послугу видачі сертифікатів, як це було раніше. Імплементаційний регламент ЄС 2024/2979 від 28 листопада 2024 року деталізує технічні вимоги та умови сертифікації засобів rQSCD, а також визначає мінімальні гарантії технологічного рівня, в тому числі за рахунок досягнення відповідності Common Criteria EAL4+ або еквіваленту згідно зі схемою SOG-IS Mutual Recognition Agreement.

Технічна реалізація mobile-first є предметом регулювання європейських та міжнародних стандартів. Основним стандартом для віддаленого підписання є CEN EN 419 241-1, який вводить функціональну модель серверного формування підпису та класифікує реалізації за рівнями контролю активації (Sole Control Assurance Levels, SCAL) [5]. CEN EN 419 241-2 окреслює вимоги до захищеного модуля активації підпису (Signature Activation Module, SAM) [6]. CEN EN 419 241-3 описує вимоги до сертифікації компонентів SAM [7]. Криптографічний модуль HSM, на якому фактично формується підпис, регулюється стандартом CEN EN 419 221-5 [8], еквівалентним FIPS 140-3 Level 3 у термінології NIST. ETSI TS 119 431-1 і TS 119 431-2 визначають вимоги до надавача послуги дистанційного підписання [9] та протоколу активації підпису [10] відповідно. ETSI EN 319 102-1 [11] і EN 319 122/132/142 деталізують формати AdES-підписів (CAdES, XAdES, PAdES). На рівні ISO/IEC ключовими є ISO/IEC 19790 (вимоги безпеки до криптографічних модулів) [12], ISO/IEC 24759 (вимоги до тестування криптографічних модулів) [13], ISO/IEC 27001-27002.

© Okhrimenko A., Stokipnyi O., Kovtun V. Analysis of the mobile-first model of qualified electronic signatures. // Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 44-50. © This is an open access article under the CC BY 4.0 International license.

Україна поступово гармонізує своє законодавство у відповідність до європейського. Прийняття Закону України «Про електронну ідентифікацію та електронні довірчі послуги» [3], а також ряду інших нормативних документів, що імплементують підходи eIDAS, відкрило можливість до віддаленого підписання та електронної ідентифікації. Проте станом на 2025 рік в Україні все ще відсутня власна повноцінна схема сертифікації кваліфікованих засобів створення підписів за Common Criteria, що актуалізує науково-практичне завдання її розбудови.

Технічна архітектура

Типове рішення на базі моделі mobile-first є розподіленою системою, у якій функції створення підпису логічно розділені між клієнтом (мобільним застосунком підписувача) та сервером (компоненти кваліфікованого надавача).

Стандарт CEN EN 419 241-1 описує два рівні контролю над активацією особистого ключа підписувача (Sole Control Assurance Level 1 (SCAL1) та Sole Control Assurance Level 2 (SCAL2)). У моделі SCAL1 рішення про активацію ключа приймає КНЕДП на підставі автентифікації підписувача. В цьому випадку сама криптографічна операція виконується автономно сервером після перевірки факту, що користувач аутентифікувався. У моделі SCAL2 ключ підпису перебуває під виключним контролем підписувача, а рішення про активацію ключа базується на використанні структури даних Signature Activation Data (SAD), що формується клієнтом і містить як автентифікаційний фактор, так і специфічну для конкретного підпису інформацію (геш документа, ідентифікатор сертифіката, час). Mobile-first архітектура для отримання статусу кваліфікованої повинна реалізовувати мінімум SCAL2, саме на цьому рівні виконується вимога eIDAS щодо виключного контролю підписувача.

Для перевірки SAD та взаємодії між сервером підписання та HSM використовується захищений програмно-апаратний компонент (Signature Activation Module, SAM). Архітектурно SAM розгортається у спеціальному сегменті захищеного периметра КНЕДП як ізольований сервіс, що виконується в захищеному середовищі (наприклад Intel SGX, AMD SEV-SNP) або як прошивка всередині самого HSM. SAM відповідає за криптографічну перевірку цілісності й автентичності SAD, перевірку відповідності SAD конкретному запиту на підпис (зв'язування SAD з хешем документа), контроль одноразовості SAD (захист від повтору), обмін авторизаційним токеном з HSM, що активує операцію SignDataAtomic над конкретним приватним ключем у HSM-сесії, ведення аудит-логів усіх спроб активації. SAM обмінюється повідомленнями з клієнтським застосунком по криптографічному протоколу Signature Activation Protocol (SAP). Вимоги до SAP визначає стандарт ETSI TS 119 431-2. Найпоширенішою реалізацією є протокол CSC API v1.0/v2.0 від Cloud Signature Consortium [15]. SAP має забезпечити непідробність авторизаційних даних, прив'язку SAD до конкретного гешу документа, одноразовість та конфіденційність.

Невід'ємною апаратною основою віддаленого кваліфікованого засобу створення підписів є HSM, в якому фізично зберігаються особисті ключі підписувачів і виконуються криптографічні операції створення підпису. HSM має відповідати CEN EN 419 221-5 (EAL4+) або FIPS 140-3 Level 3/4 [14]. Серед основних постачальників сертифікованих для довірчих послуг в ЄС HSM є Thales (Luna Network HSM), Utimaco (CryptoServer CP5), nCipher Entrust (nShield Connect XC), Atos Bull/Eviden, IBM (Crypto Express), а також ряд сертифікованих cloud-HSM сервісів AWS CloudHSM, Azure Dedicated HSM, Google Cloud HSM. Серед національних розробників криптографічних засобів слід визначити АТ "ІІТ" з ІІТ "Гряда-301" та ТОВ "САЙФЕР ПРО" з Сайфер "Шифр-HSM", які використовуються, як для побудови КНЕДП так і для побудови систем віддаленого кваліфікованого підпису. Особливістю архітектур для віддаленого підписання:

– підтримка багатокористувацької архітектури HSM через окремі логічні розділи (віртуальні захищені носії) з власними наборами політик. Така архітектура найбільш поширена серед національних КНЕДП.
– як один із варіантів архітектури є підтримка HSM захищеного зберігання великих блоків даних із зашифрованими ключами підписувачів, із неможливістю їх використання поза HSM та з можливістю їх розпакування лише в межах HSM на момент операції.
– як один із варіантів архітектури, можливість використання порогового підпису (threshold signature), коли частина підпису формується віддалено на боці HSM, а фінальне створення підпису відбувається вже на мобільному пристрої підписувача. Така архітектура використовується у національному сервісі "Дія.Підпис" разом із генерацією ключів підписувачів на короткий час дії (від кількох хвилин до кількох годин).

На стороні підписувача критичним компонентом безпеки mobile-first є захищене виконавче середовище мобільного пристрою (Secure Enclave Processor для платформ Apple, Trusted Execution Environment та StrongBox для платформ Android, eUICC для інших платформ). Криптографічні операції, що виконуються в захищеному середовищі мобільного пристрою у складі SAP, зазвичай обмежуються підписом SAD або генерацією JWT-токена.

Канал зв'язку між мобільним застосунком і серверними компонентами захищається на декількох рівнях. Захист на транспортному рівні реалізується за TLS 1.3 (IETF RFC 8446) з обмеженням наборів шифрів. Додатково до стандартного TLS застосовується:

© Okhrimenko A., Stokipnyi O., Kovtun V. Analysis of the mobile-first model of qualified electronic signatures. // Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 44-50. © This is an open access article under the CC BY 4.0 International license.

certificate pinning у клієнтському додатку (фіксація хешу конкретного сертифікату або проміжного CA); додаткове application level шифрування з використанням відкритого ключа (наприклад криптосистемою RSA чи Paillier) сервісу віддаленого підписання та сесійних симетричних ключів (наприклад AES, ChaCha20). Для серверних API критичних операцій додатково використовується взаємний TLS (mTLS) з клієнтським сертифікатом, виданим на ім'я конкретної інсталяції додатку. Поверх TLS часто реалізується додатковий шар application level шифрування на рівні застосунку, що захищає дані навіть у разі атаки MitM на TLS-рівні. Автентифікація підписувача в mobile-first QES є багатофакторною. Перший фактор (знання) реалізується через PIN, графічний ключ або пароль. Другий фактор (володіння) фактично прив'язаний до конкретного захищеного середовища мобільного пристрою (Secure Enclave чи Trusted Execution Environment), що однозначно ідентифікується через засвідчення пристрою. Третій фактор (властивість) реалізується через біометрію (відбиток пальця, обличчя, голос).

Варіанти реалізації mobile-first QES

Найпростішим та найпоширенішим варіант реалізації mobile-first КЕП є підписання на основі push-повідомлень. Підписувач ініціює дію в довільному веб-сервісі (порталі державних послуг, банківському інтерфейсі, системі електронного документообігу), сервіс надсилає запит на підпис до серверної інфраструктури кваліфікованого надавача, а надавач, у свою чергу, надсилає push-повідомлення на мобільний застосунок підписувача. Підписувач в мобільному застосунку, переглядає реквізити документа (геш, опис, ідентифікатор операції), підтверджує намір (за допомогою біометрії, PIN чи паролю), після чого клієнтський компонент формує SAD і надсилає його до SAM, який активує на HSM операцію формування підпису. Створений підпис повертається ініціатору.

Іншим поширеним варіантом є підписання на основі QR-кодів. Цей варіант використовується тоді, коли підписувач взаємодіє з веб-порталом (банк, державний сервіс) на робочій станції, який генерує QR-код з ідентифікатором сесії (та опціонально гешем документа). Підписувач сканує QR-код мобільним застосунком, який в свою чергу встановлює безпечний зв'язок з надавачем послуг віддаленого підписання, запитує авторизацію підписувача й виконує дії за протоколом SAP. Результат підписання повертається на веб-сторінку через server-sent events або long polling. Цей шаблон є комбінацією зручності робочої станції і безпеки мобільного захищеного середовища.

Федеративна реалізація моделі mobile-first КЕП передбачає розділення функції ідентифікації (через Identity Provider) та підписання (через Signing Service Provider). Підписувач автентифіковується через свого Identity Provider (банк, національну схему eID), отримує OIDC-токен, який пред'являє Signing Service Provider як доказ права на підпис. Перевага такого підходу в масштабованості через існуючі сервіси, проте основним недоліком є ризик компрометація Identity Provider, що приведе до компрометації усіх підписів користувача. Такий недолік актуалізує вимогу до додаткового підтвердження перед підписанням у самого Signing Service Provider.

Європейський гаманець цифрової ідентичності (EUDI Wallet) у моделі eIDAS 2 покликаний стати уніфікованим mobile-first контейнером для всіх кваліфікованих електронних довірчих послуг [18]. Технічно EUDI Wallet має імплементувати клієнтську частину SAP (на базі CSC API v2.0), а серверні компоненти віддаленого кваліфікованого засобу створення електронного підпису надаватимуться КНЕДП держав-членів ЄС. Українська реалізація EUDI Wallet через мобільний застосунок «Дія» стане одним з найбільш ймовірних шляхів інтеграції з європейським простором.

Перспективним є також підхід використання мобільного телефону як засобу створення КЕП. Особистий ключ підписанта зберігається безпосередньо в захищеному середовищі мобільного пристрою (Secure Enclave чи Trusted Execution Environment), а всі криптографічні операції виконується локально без використання HSM на серверній стороні. Такий підхід формально хоч і допустимий в eIDAS, проте юридичне визнання такої реалізації дуже складне. Також на практиці існує дуже обмежена кількість смартфонів, чий захищений компонент формально сертифікований за CC EAL5+.

Аналіз загроз моделі mobile-first

Одним із важливих напрямків дослідження моделі mobile-first КЕП є систематизація загроз та їх аналіз. Атаки спрямовані на різні компоненти моделі mobile-first [16].

До атак на мобільний застосунок можна віднести компрометацію операційної системи мобільного пристрою через jailbreak (iOS, iPadOS) чи root (Android), що частково або повністю нейтралізує захист Secure Enclave та Trusted Execution Environment для непривілейованих процесів. Іншими варіантами атак на мобільний застосунок є його модифікація шляхом підміни інсталяційного файлу APK/IPA, перехоплення викликів API, перехоплення PIN через кейлогери, тощо. Проти всіх відомих варіантів таких атак є ефективні методи протидії.

Іншим класом атак є атаки на захищеному середовищі мобільного пристрою. Захищене виконуюче середовище мобільного пристрою може зазнавати атак, пов'язаних з експлуатацією вразливостей Trusted Execution Environment, компрометацією Secure Enclave через bootrom-експлойти типу checkm8, атаками через витоки за побічними каналами на криптографічні модулі, а

© Okhrimenko A., Stokipnyi O., Kovtun V. Analysis of the mobile-first model of qualified electronic signatures. // Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 44-50. © This is an open access article under the CC BY 4.0 International license.

також використанням вразливостей компонентів прошивки захищеного середовища виконання.

Атаки на канал зв'язку між мобільним застосунком і серверними компонентами включають в себе перехоплення TLS трафіку через MITM з використанням ПЗ (яке додає власні кореневі сертифікати до довіреного сховища), атаки на вразливі версії TLS та атаки повтору направлені на SAD.

Атаки на серверну інфраструктуру зазвичай направлені на SAM та HSM (експлуатація вразливостей ОС та компонентів ПЗ), на СА інфраструктуру, маніпуляції чи знищення для приховування слідів в журналах аудиту.

Підписувач залишається найслабшою ланкою в моделі mobile-first КЕП. До основних класів соціально-інженерних атак відносять фішинг (через підставні веб-сайти), вішинг (переконання підписувача підтвердити операцію), атака втомою від запитів (надсилання масових push-повідомлення з метою спровокувати підтвердження без уваги до реквізитів), тощо.

Аналіз загроз моделі mobile-first

Хоча модель mobile-first КЕП має високий ступінь інженерної та регуляторної зрілості, лишаються відкритими низка фундаментальних і прикладних проблем, вирішення яких може бути перспективними науково-дослідними та інженерними задачами.

Постквантова криптографія

У серпні 2024 року NIST опублікував три фінальних стандарти постквантових алгоритмів FIPS 203 (ML-KEM, key encapsulation), FIPS 204 (ML-DSA, цифровий підпис на основі решіток) та FIPS 205 (SLH-DSA, hash-based підпис). Очікується ухвалення FIPS 206 (FN-DSA, Falcon) у 2026-2027 роках. ETSI у TS 119 312 та CEN у проєкті EN 419 241-4 готують оновлення для прийняття постквантової криптографії (PQC) у складі rQSCD. Впровадження алгоритмів PQC в модель mobile-first відкриває нові дослідницькі та інженерні задачі [17], зокрема використання гібридної схеми підписання з використанням класичних та постквантових алгоритмів, оптимізація передачі даних у зв'язку зі збільшенням розміру PQC підписів, підтримка PQC на рівні прошивок HSM та клієнтських мобільних пристроїв, підвищення швидкодії PQC операцій.

Розділене зберігання ключа

Модель mobile-first передбачає зберігання повного особистого ключа або в HSM серверної сторони, або в захищеній зоні мобільного пристрою. Threshold signature пропонує проміжний підхід, у якій ключ математично розділений між двома (або більше) сторонами без можливості реконструкції повного ключа жодною з них одноосібно або взагалі реконструкція не передбачається самим протоколом (multi part computation чи secure computation). Підпис обчислюється через спільний багатоетапний протокол. Навіть повна компрометація серверної інфраструктури не виявляє повного ключа, оскільки частини ключа зберігається в інших місцях. Використання такого підходу потребуватиме доведення юридичної вимоги виключного контролю ключа в розумінні eIDAS.

Zero-knowledge attestation для SAM

Кваліфікований надавач, експлуатуючи SAM, має забезпечити аудитованість усіх операцій активації підпису. Однак повний аудит-лог містить чутливу інформацію. Zero-knowledge protocols (zk-SNARK, zk-STARK, zkBoo+) дозволяють надавачу публічно довести коректність операції активації без розкриття самого SAD або змісту документа. Доведення ефективності zk-доказів коректності SAP-операцій з обмеженнями часу, використання технологій blockchain та технологій розподіленого реєстру (DLT) в якості захищеного від несанкціонованого втручання журналу, вибір балансу прозорості та конфіденційності будуть актуальними задачами.

DLT як надавач кваліфікованих позначок часу й архівації

Використання технологій розподіленого реєстру (DLT, blockchain) в якості захищеного від несанкціонованого втручання журналу, аналогу timestamp authority та як компоненту кваліфікованої електронної архівної послуги. Питання, які виникнуть в цьому випадку, будуть пов'язані з досліженням і підвищенням швидкодії операцій при використанні публічних і приватних реєстрів, проблемою визнання позначок часу отриманих на основі роботи DLT у відповідності до ETSI EN 319 421, правова рамка визнання DLT-зафіксованої позначки часу в судочинстві.

Висновки

У результаті проведеного аналізу встановлено, що модель mobile-first КЕП стала домінуючим підходом до надання кваліфікованих електронних довірчих послуг у Європейському Союзі та Україні. Основною причиною її поширення є можливість поєднання високого рівня юридичної значущості електронного підпису із зручністю використання мобільних пристроїв як основного інтерфейсу взаємодії користувача з цифровими сервісами.

Дослідження показало, що сучасна mobile-first модель базується на архітектурі віддаленого кваліфікованого засобу створення підпису (remote QSCD), у якій особистий ключ підписувача зберігається у захищеній серверній інфраструктурі КНЕДП, а мобільний застосунок виконує функції автентифікації, активації підпису та підтвердження волевиявлення користувача. Ключову роль у забезпеченні вимоги виключного контролю підписувача відіграють механізми SCAL2, SAD, SAM, а також використання

HSM та захищених середовищ виконання мобільних пристроїв.

Встановлено, що розвиток нормативної бази ЄС, зокрема Регламентів eIDAS та eIDAS 2, створив повноцінні юридичні передумови для легітимізації віддаленого підписання та формування окремої кваліфікованої послуги remote QSCD management. Водночас в Україні, попри поступову гармонізацію законодавства з європейськими вимогами, залишається актуальною проблема відсутності національної схеми сертифікації QSCD за Common Criteria.

Проаналізовано основні архітектурні варіанти реалізації mobile-first підписання, серед яких push-модель, QR-модель, федеративна модель та інтеграція з EUDI Wallet. Визначено, що найбільш перспективним напрямком розвитку є інтеграція mobile-first КЕП із Європейським гаманцем цифрової ідентичності та сервісами транскордонної електронної ідентифікації.

Окрему увагу приділено систематизації загроз моделі mobile-first. Встановлено, що критичними залишаються ризики компрометації мобільного пристрою, атак на Trusted Execution Environment та Secure Enclave, соціальної інженерії, MITM-атак на канали зв'язку, а також компрометації серверної інфраструктури SAM/HSM. При цьому підписувач залишається найбільш вразливою складовою всієї системи.

Перспективними напрямками подальших наукових та інженерних досліджень визначено впровадження постквантової криптографії у mobile-first архітектури, використання threshold cryptography для розділеного зберігання ключів, застосування zero-knowledge attestation для аудитованості SAM, а також інтеграцію DLT/blockchain-технологій у сервіси кваліфікованих позначок часу та електронного архівування.

Список використаних джерел

[1]. European Parliament, Council of the European Union. 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 repealing Directive 1999/93/EC // Official Journal of the European Union. – 2014. – L 257. – P. 73–114.

[2]. European Parliament, Council of the European Union. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework // Official Journal of the European Union. – 2024. – L 2024/1183.

[3]. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII від 05.10.2017 // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 400.

[4]. European Commission. Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Article 30(3) and Article 39(2) of Regulation (EU) No 910/2014 // Official Journal of the European Union. – 2016. – L 109. – P. 40–42.

[5]. CEN EN 419 241-1:2018. Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements. – Brussels: European Committee for Standardization (CEN), 2018.

[6]. CEN EN 419 241-2:2019. Trustworthy Systems Supporting Server Signing – Part 2: Protection Profile for QSCD for Server Signing. – Brussels: European Committee for Standardization (CEN), 2019.

[7]. CEN EN 419 241-3:2019. Trustworthy Systems Supporting Server Signing – Part 3: Protection Profile for Signature Activation Module for Server Signing. – Brussels: European Committee for Standardization (CEN), 2019.

[8]. CEN EN 419 221-5:2018. Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services. – Brussels: European Committee for Standardization (CEN), 2018.

[9]. ETSI. ETSI TS 119 431-1 V1.2.1 (2023-07). Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers Supporting Server Signing.

[10]. ETSI. ETSI TS 119 431-2 V1.2.1 (2023-07). Electronic Signatures and Infrastructures (ESI); Protocols for Remote Digital Signature Creation.

[11]. ETSI. ETSI EN 319 102-1 V1.4.1 (2024-01). Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures.

[12]. International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 19790:2012. Security Requirements for Cryptographic Modules. – Geneva: ISO/IEC, 2012.

[13]. International Organization for Standardization, International Electrotechnical Commission. ISO/IEC 24759:2017. Test Requirements for Cryptographic Modules. – Geneva: ISO/IEC, 2017.

[14]. National Institute of Standards and Technology. FIPS 140-3. Security Requirements for Cryptographic Modules. – Gaithersburg: NIST, 2019.

[15]. Cloud Signature Consortium. CSC API Specification Version 2.0. – 2023.

[16]. ENISA. Remote Identity Proofing and Trust Services Security Recommendations. – Heraklion: ENISA, 2023.

[17]. ENISA. Post-Quantum Cryptography: Current State and Quantum Mitigation. – Heraklion: ENISA, 2024.

[18]. European Commission. Architecture and Reference Framework for the European Digital Identity Wallet. Version 1.4.0. – Brussels: European Commission, 2025.

[19]. Центральний засвідчувальний орган. Оцінка стану розвитку сфери електронних довірчих послуг. – URL: https://czo.gov.ua/development

[20]. European Commission. EU/EEA Trusted List Browser. – URL: https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls

УДК 004.056

A. Okhrimenko, O.Stokipnyi, V. Kovtun. Analysis of the mobile-first model of qualified electronic signatures

Abstract. *The article provides a comprehensive analysis of the mobile-first qualified electronic signature (QES) model in the context of modern trust services. The regulatory framework of remote QSCD operation according to eIDAS and eIDAS 2 requirements, as well as the harmonization of Ukrainian legislation with the European regulatory framework, are examined. The technical architecture of mobile-first signing is analyzed, including SCAL2 mechanisms, Signature Activation Data (SAD), Signature Activation Module (SAM),*

© Okhrimenko A., Stokipnyi O., Kovtun V. Analysis of the mobile-first model of qualified electronic signatures. // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 44-50. © This is an open access article under the CC BY 4.0 International license.*

Hardware Security Module (HSM), Trusted Execution Environment (TEE), and Secure Enclave technologies. The main implementation models of mobile-first QES are considered, including push-based, QR-based, federated architectures, and integration with the EUDI Wallet ecosystem. A systematic analysis of threats targeting mobile applications, secure execution environments, server infrastructure, and communication channels is conducted. Prospective research directions are identified, including post-quantum cryptography integration, threshold cryptography, zero-knowledge attestation mechanisms, and distributed ledger technologies for trust services and electronic archiving.

Keywords: *qualified electronic signature, mobile-first, remote QSCD, eIDAS, trust services, Signature Activation Module, Hardware Security Module, post-quantum cryptography, EUDI Wallet.*

ОХРІМЕНКО Андрій, кандидат технічних наук, старший викладач кафедри системного аналізу та інформаційних технологій Маріупольського державного університету.
Andrii Okhrimenko, PhD, Senior Lecturer at the Department of Systems Analysis and Information Technologies, Mariupol State University.

СТОКІПНИЙ Олександр, кандидат технічних наук, доцент кафедри інтелектуальних кібернетичних систем Національний університету «Київський авіаційний інститут».
Oleksandr Stokipnyi, PhD, Associate Professor at the Department of Intelligent Cybernetic Systems, National University "Kyiv Aviation Institute".

КОВТУН Владислав, кандидат технічних наук, доцент кафедри програмної інженерії та інтелектуальних технологій управління Національного технічного університету «Харківський політехнічний інститут».
Vladyslav Kovtun, PhD, Associate Professor at the Department of Software Engineering and Intelligent Management Technologies, National Technical University "Kharkiv Polytechnic Institute".

Дата надходження:	Дата прийняття:	Дата публікації:
18.06.2026	17.07.2026	21.08.2026