ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від ____ _____ 2026 р. № _____

ЗМІНИ,

що вносяться до постанов Кабінету Міністрів України

1. У вимогах до надавачів послуг електронної ідентифікації та електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 28 червня 2024 р. № 764 (Офіційний вісник України, 2024 р., № 63, ст. 3762):

1) пункт 4 викласти в такій редакції:

“4. Інші терміни вживаються у значенні, наведеному в Законах України “Про захист інформації в інформаційно-комунікаційних системах”, “Про акредитацію органів з оцінки відповідності”, “Про електронні документи та електронний документообіг”, “Про регулювання містобудівної діяльності”, “Про технічні регламенти та оцінку відповідності”, “Про електронну ідентифікацію та електронні довірчі послуги”, “Про основні засади забезпечення кібербезпеки України”, “Про електронні комунікації”, постанові Кабінету Міністрів України від 11 серпня 2023 р. № 844 “Про затвердження вимог до Довірчого списку” (Офіційний вісник України, 2023 р., № 79, ст. 4487), постанові Кабінету Міністрів України від 13 вересня 2024 р. № 1062 “Деякі питання акредитації органів з оцінки відповідності та проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг” (Офіційний вісник України, 2024 р., № 86, ст. 5358) та інших нормативно-правових актах у сферах електронної ідентифікації та електронних довірчих послуг.”;

2) абзаци третій – п’ятий пункту 5 викласти в такій редакції:

“ДСТУ ETSI EN 319 412-1:2026 (ETSI EN 319 412-1 V1.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та загальні структури даних”;

ДСТУ ETSI EN 319 412-2:2026 (ETSI EN 319 412-2 V2.4.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 2. Профіль сертифіката для сертифікатів, виданих фізичним особам”;

ДСТУ ETSI EN 319 412-3:2026 (ETSI EN 319 412-3 V1.3.1 (2023-09), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 3. Профіль сертифіката для сертифікатів, виданих юридичним особам”;

3) абзаци другий – п’ятий пункту 15 викласти в такій редакції:

“ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”;

ДСТУ ETSI EN 319 411-1:2026 (ETSI EN 319 411-1 V1.5.1 (2025-04), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги”;

ДСТУ ETSI EN 319 411-2:2026 (ETSI EN 319 411-2 V2.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС”;

ДСТУ ETSI EN 319 421:2026 (ETSI EN 319 421 V1.3.1 (2025-07), IDT) “Електронні підписи та інфраструктури (ESI). Політика та вимоги безпеки щодо надавачів довірчих послуг, які видають часові штемпелі”.”;

4) пункт 24 викласти в такій редакції:

“24. Структура та зміст регламенту, зокрема політики сертифіката та положень сертифікаційних практик, визначаються з урахуванням ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг” та ДСТУ ETSI EN 319 411-1:2026 (ETSI EN 319 411-1 V1.5.1 (2025-04), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги”.”;

5) пункт 30 доповнити новим абзацом такого змісту:

“Особливості застосування під час надання електронних довірчих послуг стандартів, визначених цими вимогами, встановлюються технічними специфікаціями, затвердженими Мінцифри.”;

6) абзац третій пункту 31 викласти в такій редакції:

“ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”;”;

7) пункт 32 викласти в такій редакції:

“32. Ідентифікація заявника та перевірка обсягу його цивільної правоздатності та дієздатності здійснюються відповідно до вимог статті 22 Закону, Порядку проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи − підприємця під час надання електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 28 червня 2024 р. № 764 “Деякі питання електронної ідентифікації та електронних довірчих послуг”, та з урахуванням ДСТУ ETSI EN 319 411-1:2026 (ETSI EN 319 411-1 V1.5.1 (2025-04), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги”, та ДСТУ ETSI EN 319 411-2:2026 (ETSI EN 319 411-2 V2.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих

послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС”;

8) пункт 43 викласти в такій редакції:

“43. Кваліфіковані сертифікати відкритих ключів, що формуються кваліфікованими надавачами довірчих послуг, центральним засвідчувальним органом, засвідчувальним центром під час надання кваліфікованих електронних довірчих послуг, повинні відповідати вимогам, установленим частинами першою – п’ятою статті 23 Закону, а також формуватися з дотриманням стандартів, визначених пунктом 5 цих вимог, та ДСТУ ETSI EN 319 412-5:2026 (ETSI EN 319 412-5 V2.5.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 5. Заяви про якість”.

У разі якщо особистий ключ, що відповідає кваліфікованому сертифікату відкритого ключа, створюється та зберігається в засобі кваліфікованого електронного підпису чи печатки, сертифікованому органом із сертифікації, уповноваженим або призначеним відповідно до законодавства Європейського Союзу для проведення сертифікації таких засобів, такий кваліфікований сертифікат відкритого ключа повинен містити передбачені підпунктом 4.2.2 пункту 4.2 розділу 4 ДСТУ ETSI EN 319 412-5:2026 (ETSI EN 319 412-5 V2.5.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 5. Заяви про якість” відомості про те, що особистий ключ, пов’язаний із зазначеним у сертифікаті відкритим ключем, зберігається в такому засобі.”;

9) абзац четвертий пункту 56 викласти в такій редакції:

“ Контролюючий орган може подати запит до органу з оцінки відповідності про надання звіту про оцінку відповідності, складеного за результатами проведення процедури оцінки відповідності.”;

10) абзаци другий, третій пункту 62 викласти в такій редакції:

“ДСТУ ETSI EN 319 411-1:2026 (ETSI EN 319 411-1 V1.5.1 (2025-04), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги”;

ДСТУ ETSI EN 319 411-2:2026 (ETSI EN 319 411-2 V2.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС”;

11) пункт 74 доповнити новими абзацами такого змісту:

“Для надання кваліфікованої електронної довірчої послуги формування кваліфікованих сертифікатів електронного підпису або електронної печатки відповідно до відомостей, внесених до кожного окремого файла Довірчого списку, кваліфікований надавач довірчих послуг використовує окрему пару ключів та відповідний їй кваліфікований сертифікат відкритого ключа.

Усі кваліфіковані сертифікати електронного підпису або електронної печатки користувачів електронних довірчих послуг, що формуються під час надання такої послуги відповідно до відомостей певного файла Довірчого списку, формуються з використанням особистого ключа відповідної пари ключів.”;

12) пункт 75 доповнити новими абзацами такого змісту:

“Для надання кваліфікованих електронних довірчих послуг, відомості про які внесені до різних файлів Довірчого списку, кваліфікований надавач довірчих послуг використовує різні відкриті ключі та відповідні їм кваліфіковані сертифікати відкритих ключів.

Під час формування кваліфікованого сертифіката відкритого ключа кваліфікованого надавача довірчих послуг центральний засвідчувальний орган або засвідчувальний центр перевіряє, чи використовується відкритий ключ, зазначений у запиті на формування такого сертифіката, під час надання кваліфікованої електронної довірчої послуги, відомості про яку внесені до іншого файла Довірчого списку.

Центральний засвідчувальний орган або засвідчувальний центр не здійснює засвідчення чинності відкритого ключа, зазначеного у запиті на формування кваліфікованого сертифіката відкритого ключа кваліфікованого надавача довірчих послуг, якщо за результатами перевірки встановлено, що відкритий ключ, зазначений у цьому запиті, використовується під час надання кваліфікованої електронної довірчої послуги, відомості про яку внесені до іншого файла Довірчого списку.”;

13) абзаци другий, третій пункту 77 викласти в такій редакції:

“ДСТУ ETSI EN 319 411-1:2026 (ETSI EN 319 411-1 V1.5.1 (2025-04), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги”;

ДСТУ ETSI EN 319 411-2:2026 (ETSI EN 319 411-2 V2.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС”;”

14) абзаци другий, третій пункту 88 викласти в такій редакції:

“ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”;

ДСТУ ETSI EN 319 421:2026 (ETSI EN 319 421 V1.3.1 (2025-07), IDT) “Електронні підписи та інфраструктури (ESI). Політика та вимоги безпеки щодо надавачів довірчих послуг, які видають часові штемпелі”;”

15) у пункті 100:

підпункт 2 викласти в такій редакції:

“2) зміни у складі інформаційно-комунікаційної системи кваліфікованого надавача довірчих послуг, які впливають або можуть вплинути на відповідність кваліфікованого надавача довірчих послуг вимогам, відповідність яким підтверджено у звіті про оцінку відповідності;”;

підпункт 4 викласти в такій редакції:

“4) проходження кваліфікованим надавачем довірчих послуг процедури оцінки відповідності в разі модернізації апаратного, апаратно-програмного пристрою чи програмного забезпечення, що входять до складу програмно-технічного комплексу, та надання звіту про оцінку відповідності, складеного за результатами такої процедури;”;

16) у пункті 102:

абзац чотирнадцятий викласти в такій редакції:

“ДСТУ ETSI TS 119 431-1:2026 (ETSI TS 119 431-1 V1.3.1 (2024-12), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг. Частина 1. Послуги TSP, що працюють з віддаленим QSCD/SCDev”;”;

абзац сімнадцятий викласти в такій редакції:

“ДСТУ ETSI TS 119 495:2026 (ETSI TS 119 495 V1.8.1 (2026-04), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги до специфічних секторів. Профілі сертифікатів та вимоги щодо політики TSP для відкритого банкінгу”;”;

17) доповнити новими вимогами такого змісту:

“Вимоги до кваліфікованих надавачів довірчих послуг та кваліфікованих електронних довірчих послуг, що ними надаються, відомості про які внесені до файлу Довірчого списку TL-UA-EC

106. Кваліфіковані надавачі довірчих послуг, відомості про яких та про кваліфіковані електронні довірчі послуги, що ними надаються, внесені до файлу Довірчого списку TL-UA-EC повинні дотримуватися таких стандартів щодо відповідних кваліфікованих електронних довірчих послуг:

1) для кваліфікованої електронної довірчої послуги формування кваліфікованих сертифікатів електронного підпису застосовуються пункти 5.2, 6.1, 6.4, 6.5, 6.8 та 6.9 ДСТУ ETSI EN 319 411-2:2026 (ETSI EN 319 411-2 V2.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС”;

2) для кваліфікованої електронної довірчої послуги формування кваліфікованих сертифікатів електронної печатки застосовуються пункти 5.2, 6.1, 6.4, 6.5, 6.8 та 6.9 ДСТУ ETSI EN 319 411-2:2026 (ETSI EN 319 411-2 V2.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо

політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС";

3) для кваліфікованої електронної довірчої послуги формування кваліфікованої електронної позначки часу застосовуються пункти 5, 6 та 7 ДСТУ ETSI EN 319 421:2026 (ETSI EN 319 421 V1.3.1 (2025-07), IDT) "Електронні підписи та інфраструктури (ESI). Політика та вимоги безпеки щодо надавачів довірчих послуг, які видають часові штемпелі".

Кваліфікований надавач довірчих послуг під час надання кваліфікованої електронної довірчої послуги формування кваліфікованих сертифікатів електронного підпису або електронної печатки, відомості про яку внесені до файлу Довірчого списку TL-UA-EC, забезпечує, щоб кожний сформований під час надання такої послуги кваліфікований сертифікат електронного підпису або електронної печатки містив об'єктний ідентифікатор (OID) політики сертифіката, визначений Мінцифри в межах реалізації вимог стандартів, у тому числі щодо забезпечення сумісності.

Зазначені стандарти застосовуються з урахуванням технічних специфікацій, у тому числі щодо забезпечення сумісності, затверджених Мінцифри відповідно до законодавства у сфері електронних довірчих послуг.

Кваліфіковані надавачі довірчих послуг, які здійснюють встановлення особи повністю автоматизованим способом, встановлюють та підтримують цільові значення показника хибного прийняття (FAR) та показника хибної відмови (FRR) для такого процесу на основі аналізу ризиків, проведеного відповідно до пункту 107 цих вимог. Такі цільові значення повинні бути не вищими за відповідні цільові значення, установлені для процесів встановлення особи, що поєднують автоматизовані операції та перевірку уповноваженим працівником, у разі встановлення таких значень для відповідних процесів.

У разі розбіжностей між положеннями стандартів, зазначених у цьому пункті, та вимогами, встановленими у пунктах 108–111 цих вимог, застосовуються вимоги, встановлені у пунктах 108–111 цих вимог.

107. Кваліфікований надавач довірчих послуг створює та підтримує систему управління ризиками, пов'язаними з наданням кваліфікованих електронних довірчих послуг, яка охоплює юридичні, комерційні, операційні та інші прямі або непрямі ризики.

Політики управління ризиками чітко визначають кваліфіковані електронні довірчі послуги, до яких вони застосовуються, є специфічними для відповідних послуг і затверджуються керівником кваліфікованого надавача довірчих послуг, а якщо таким надавачем є фізична особа − підприємець, − такою особою. Політики управління ризиками включають щонайменше:

загальний рівень толерантності до ризику відповідно до критичності та необхідного рівня безпеки кваліфікованих електронних довірчих послуг з урахуванням новітніх технологічних розробок;

критерії ризику, включаючи щонайменше ймовірність, вплив та рівень ризику, з урахуванням даних про кіберзагрози та вразливості;

підхід до ідентифікації та документування ризиків для надання послуг з урахуванням повного обсягу інформаційно-комунікаційної системи кваліфікованого надавача довірчих послуг, включаючи ризики, пов'язані з компонентами такої системи та будь-якими активними або пасивними сторонами, залученими до впровадження системи або надання послуг;

процес оцінювання ідентифікованих ризиків на основі визначених критеріїв ризику;

процес ідентифікації, пріоритезації та безперервного моніторингу впровадження заходів з оброблення ризиків;

процес безперервного моніторингу впровадження політик управління ризиками.

Кваліфікований надавач довірчих послуг установлює процедури та веде документацію, необхідні для забезпечення дотримання вимог законодавства, що застосовуються до надання кваліфікованих електронних довірчих послуг, а також установлює документовані процедури проведення моніторингу змін у законодавстві України та Європейського Союзу, що можуть вплинути на надання таких послуг.

Кваліфікований надавач довірчих послуг ідентифікує, документує та оцінює ризики відповідно до політик управління ризиками, зокрема ідентифікує ризики, пов'язані з третіми сторонами, та потенційні єдині точки відмови у наданні послуг.

Заходи з оброблення ризиків плануються, документуються та впроваджуються відповідно до політик управління ризиками. Кваліфікований надавач довірчих послуг:

ідентифікує та пріоритезує заходи з оброблення ризиків;

обирає, затверджує та документує обрані заходи, включаючи вимоги безпеки та операційні процедури, у плані оброблення ризиків, у якому визначаються особи, відповідальні за впровадження таких заходів, та строки їх впровадження;

здійснює безперервний моніторинг впровадження заходів з оброблення ризиків.

Значним інцидентом є інцидент, пов'язаний з наданням електронної довірчої послуги, що відповідає хоча б одному з таких критеріїв:

кваліфікована електронна довірча послуга є повністю недоступною понад 20 хвилин;

кваліфікована електронна довірча послуга є недоступною користувачам електронних довірчих послуг або особам, які покладаються на результати її надання, загалом понад одну годину протягом календарного тижня;

обмежена доступність кваліфікованої електронної довірчої послуги впливає на понад 1 відсоток зазначених осіб або понад 200 000 таких осіб залежно від того, яке значення є меншим;

порушено фізичний доступ або захист фізичного доступу до зони, в якій розміщені інформаційно-комунікаційні системи та доступ до якої дозволено лише уповноваженим працівникам кваліфікованого надавача довірчих послуг;

порушено цілісність, конфіденційність або автентичність даних, що зберігаються, передаються чи обробляються у зв'язку з наданням кваліфікованої електронної довірчої послуги, якщо це впливає на понад 0,1 відсотка зазначених осіб або понад 100 таких осіб залежно від того, яке значення є меншим.

Планові перерви у наданні кваліфікованої електронної довірчої послуги та передбачувані наслідки планового технічного обслуговування не вважаються значними інцидентами.Під час ідентифікації, вибору, затвердження та пріоритезації заходів з оброблення ризиків враховуються:

результати оцінювання ризиків;

ефективність заходів з оброблення ризиків;

результати оцінки відповідності;

значні інциденти;

співвідношення витрат на впровадження заходів з оброблення ризиків та очікуваної користі від їх впровадження;

відповідна класифікація активів;

результати аналізу впливу ідентифікованих ризиків на діяльність кваліфікованого надавача довірчих послуг.

План оброблення ризиків повинен містити обґрунтування прийняття ризиків, що залишаються після впровадження заходів з їх оброблення. Такі ризики затверджуються керівником кваліфікованого надавача довірчих послуг, а якщо таким надавачем є фізична особа − підприємець, − такою особою.

Результати оцінювання ризиків та план оброблення ризиків переглядаються, документуються та за потреби оновлюються із запланованою періодичністю, але не рідше одного разу на рік, а також у разі змін в інфраструктурі, діяльності чи ризиках, що можуть вплинути на результати оцінювання ризиків або план їх оброблення, або значних інцидентів.

Кваліфікований надавач довірчих послуг забезпечує доступність, цілісність та конфіденційність інформації, що зберігається ним для забезпечення доказів у судових провадженнях та безперервності надання кваліфікованих електронних довірчих послуг.

108. Кваліфіковані надавачі довірчих послуг, відомості про яких та про кваліфіковані електронні довірчі послуги, що ними надаються, внесені до файлу Довірчого списку TL-UA-EC, повідомляють центральний засвідчувальний орган, а у разі коли відомості про такого надавача внесені до Довірчого списку за поданням засвідчувального центру, – засвідчувальний центр у таких випадках:

1) про намір розпочати надання кваліфікованої електронної довірчої послуги − не пізніше ніж за три місяці до запланованої дати початку її надання;

2) про намір впровадити зміни в наданні кваліфікованої електронної довірчої послуги − не пізніше ніж за один місяць до впровадження таких змін;

3) про намір припинити надання однієї чи декількох кваліфікованих електронних довірчих послуг, відомості про які внесені до файлу Довірчого списку TL-UA-EC, − не пізніше ніж за три місяці до запланованої дати припинення їх надання.

Повідомлення подаються центральному засвідчувальному органу через програмний інтерфейс інформаційно-комунікаційної системи центрального засвідчувального органу, а засвідчувальному центру — на адресу електронної пошти Національного банку України або через систему електронної взаємодії органів виконавчої влади або систему електронної пошти Національного банку України.

Повідомлення, передбачені підпунктами 2 і 3 цього пункту, також подаються органу з оцінки відповідності, який видав чинний сертифікат відповідності щодо відповідної кваліфікованої електронної довірчої послуги.

Повідомлення, зазначене в підпункті 3 цього пункту, не звільняє кваліфікованого надавача довірчих послуг від виконання обов'язків, визначених статтею 31 Закону, у разі прийняття рішення про припинення надання кваліфікованих електронних довірчих послуг.

До змін у наданні кваліфікованої електронної довірчої послуги, про намір впровадити які подається повідомлення відповідно до підпункту 2 цього пункту, належать зміни щодо:

опису кваліфікованої електронної довірчої послуги, регламенту роботи кваліфікованого надавача довірчих послуг, політики сертифіката, положень сертифікаційних практик або умов надання відповідної кваліфікованої електронної довірчої послуги;

інформаційно-комунікаційних систем та програмно-технічних комплексів, що використовуються для надання електронних довірчих послуг;

розміщення технічних компонентів або місця надання технічних послуг, необхідних для надання кваліфікованих електронних довірчих послуг;

використання методів криптографічного та технічного захисту інформації під час надання кваліфікованих електронних довірчих послуг;

способів реєстрації та ідентифікації осіб, які звертаються за отриманням кваліфікованої електронної довірчої послуги;

організаційної структури або системи управління кваліфікованого надавача довірчих послуг;

плану припинення діяльності з надання кваліфікованих електронних довірчих послуг (далі − план припинення);

страхування відповідальності або поповнення/списання коштів на поточному рахунку із спеціальним режимом використання в банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів, або

рахунку в Національному банку − для банків − кваліфікованих надавачів довірчих послуг, кваліфікованого надавача довірчих послуг, створеного Національним банком) для забезпечення відшкодування збитків, які можуть бути заподіяні кваліфікованим надавачем довірчих послуг користувачам електронних довірчих послуг внаслідок неналежного виконання своїх обов’язків;

відомостей, що містяться у файлі Довірчого списку TL-UA-EC;

третіх сторін, залучених до надання кваліфікованої електронної довірчої послуги, в тому числі, відокремлених пунктів реєстрації, а також умов договорів з такими третіми сторонами.

Повідомлення, передбачене підпунктом 2 цього пункту, повинно містити:

опис зміни;

заплановану дату та час впровадження зміни;

причини зміни та документи, що підтверджують такі причини (за наявності);

оновлені документи, яких стосується зміна (за наявності).

109. Кваліфікований надавач довірчих послуг розробляє план припинення, що визначає заходи та процедури припинення надання кожної кваліфікованої електронної довірчої послуги, відомості про яку внесені до файлу Довірчого списку TL-UA-EC, або її частини, зокрема заходи щодо зберігання та забезпечення доступності документованої інформації, створеної або отриманої під час надання відповідної послуги.

Кваліфікований надавач довірчих послуг встановлює механізми контролю та процедури для забезпечення доступності для внутрішнього використання регламенту роботи кваліфікованого надавача довірчих послуг (політика сертифіката, положення сертифікаційних практик та інші документи, що визначають правила і процедури надання електронних довірчих послуг), договорів, укладених з третіми сторонами, та інших документів, необхідних для забезпечення виконання плану припинення.

Кваліфікований надавач довірчих послуг забезпечує актуальність плану припинення та пов’язаних з ним документів.

Кваліфікований надавач довірчих послуг переглядає план припинення та будь-які пов'язані з ним документи щонайменше кожні два роки, а також у разі впровадження будь-яких змін у діяльності кваліфікованого надавача довірчих послуг або в наданні кваліфікованих електронних довірчих послуг, відомості про які внесені до файлу Довірчого списку TL-UA-EC.

Кваліфікований надавач довірчих послуг здійснює управління ризиками, пов’язаними з припиненням надання відповідної кваліфікованої електронної довірчої послуги, як складову системи управління ризиками, зазначеної в пункті 107 цих вимог, з урахуванням ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки”, а у разі якщо

припинення надання відповідної кваліфікованої електронної довірчої послуги пов’язане з використанням засобів електронної ідентифікації, − також з урахуванням Порядку оцінки ризиків і наслідків неправомірного використання чи підміни ідентифікаційних даних користувачів послуг електронної ідентифікації та інформування контролюючого органу про надання електронних довірчих послуг з використанням засобів електронної ідентифікації, затвердженого постановою Кабінету Міністрів України від 28 лютого 2025 р. № 226 (Офіційний вісник України, 2025 р., № 26, ст. 1725).

Кваліфікований надавач довірчих послуг забезпечує наявність фінансових ресурсів, необхідних для виконання плану припинення, зокрема шляхом укладення договору страхування відповідальності або забезпечення наявності коштів на поточному рахунку із спеціальним режимом використання в банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів, або рахунку в Національному банку − для банків − кваліфікованих надавачів довірчих послуг, кваліфікованого надавача довірчих послуг, створеного Національним банком) для забезпечення відшкодування збитків, які можуть бути заподіяні кваліфікованим надавачем довірчих послуг користувачам електронних довірчих послуг внаслідок неналежного виконання своїх обов’язків, у тому числі у разі неочікуваного припинення надання однієї або декількох кваліфікованих електронних довірчих послуг.

Кваліфікований надавач довірчих послуг забезпечує, щоб план припинення та пов’язані з ним документи містили положення щодо:

1) припинення надання відповідної кваліфікованої електронної довірчої послуги, зокрема припинення експлуатації будь-яких технічних компонентів або технічних послуг, що використовуються для надання відповідної кваліфікованої електронної довірчої послуги;

2) своєчасного оновлення відомостей про відповідні послуги, які внесені до файлу Довірчого списку TL-UA-EC;

3) блокування, скасування кваліфікованих сертифікатів відкритих ключів, виданих до припинення кваліфікованої електронної довірчої послуги з формування кваліфікованих сертифікатів відкритих ключів, крім випадків, коли відповідні права та обов’язки кваліфікованого надавача довірчих послуг щодо відповідної послуги передаються іншому кваліфікованому надавачу довірчих послуг у спосіб, який забезпечує безперервність надання такої послуги;

4) неможливості після припинення надання кваліфікованої електронної довірчої послуги використовувати особистий ключ кваліфікованого надавача довірчих послуг для подальшого надання такої послуги;

5) забезпечення доступності та придатності до використання всієї відповідної документованої інформації, що зберігається кваліфікованим надавачем довірчих послуг;

6) варіантів запланованого, незапланованого, часткового та повного припинення;

7) забезпечення захисту інтересів користувачів електронних довірчих послуг після припинення надання відповідної кваліфікованої електронної довірчої послуги, зокрема шляхом подальшого підтримання в належному стані інформації, необхідної користувачам для перевірки чинності результатів надання такої послуги;

8) укладення договорів або здійснення інших заходів, необхідних для забезпечення безперервності надання кваліфікованої електронної довірчої послуги;

9) повідомлення користувачів електронних довірчих послуг, центрального засвідчувального органу або засвідчувального центру та контролюючого органу про припинення надання відповідної кваліфікованої електронної довірчої послуги.

110. Процедури та заходи, зазначені в підпункті 5 пункту 109 цих вимог, повинні забезпечувати доступність та придатність до використання документованої інформації, необхідної для:

1) надання доказів у судових провадженнях щодо відповідності надання кваліфікованих електронних довірчих послуг вимогам законодавства у сферах електронної ідентифікації та електронних довірчих послуг, а також законодавства про захист персональних даних;

2) забезпечення можливості перевірки чинності кваліфікованих електронних підписів, кваліфікованих електронних печаток, кваліфікованих електронних позначок часу кваліфікованого надавача довірчих послуг, а також постійного зберігання всіх виданих кваліфікованих сертифікатів відкритих ключів після припинення надання відповідної кваліфікованої електронної довірчої послуги.

111. Кваліфікований надавач довірчих послуг забезпечує, щоб пов’язані з планом припинення документи містили таку інформацію:

1) порядок припинення кваліфікованих електронних довірчих послуг;

2) результати внутрішніх перевірок, внутрішнього аудиту та оцінки виконання плану припинення;

3) звіти про оцінку відповідності, що стосуються плану припинення;

4) порядок припинення правовідносин з третіми сторонами, зокрема відокремленими пунктами реєстрації, залученими до надання кваліфікованої електронної довірчої послуги, надання якої підлягає припиненню;

5) регламент роботи кваліфікованого надавача довірчих послуг (політика сертифіката, положення сертифікаційних практик та інші документи, що визначають правила і процедури надання електронних довірчих послуг).

Вимоги до внесення відомостей про кваліфікованих надавачів довірчих послуг та кваліфіковані електронні довірчі послуги, що ними надаються, до файлу Довірчого списку TL-UA-EC

112. Для внесення відомостей про юридичних осіб та фізичних осіб − підприємців, які мають намір надавати кваліфіковані електронні довірчі послуги, кваліфікованих надавачів довірчих послуг та кваліфікованих електронних довірчих послуг, що ними надаються або мають надаватися, до файлу Довірчого списку TL-UA-EC, відповідна юридична особа, фізична особа - підприємець або кваліфікований надавач довірчих послуг отримує та подає до центрального засвідчувального органу або засвідчувального центру звіт про оцінку відповідності, виданий органом з оцінки відповідності, акредитованим національним органом з акредитації держави − члена Європейського Союзу, а також відомості та документи, перелік яких визначено у пункті 115 цих вимог.

113. Звіт про оцінку відповідності повинен підтверджувати, що кваліфікований надавач довірчих послуг або особа, яка має намір надавати кваліфіковані електронні довірчі послуги, а також відповідні кваліфіковані електронні довірчі послуги відповідають вимогам до кваліфікованих надавачів електронних довірчих послуг та кваліфікованих електронних довірчих послуг, що ними надаються, встановленим Регламентом (ЄС) № 910/2014 Європейського Парламенту і Ради від 23 липня 2014 р. про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС (далі − Вимоги ЄС).

Звіт про оцінку відповідності щодо кваліфікованої електронної довірчої послуги формування кваліфікованих сертифікатів електронного підпису або електронної печатки повинен окремо підтверджувати дотримання вимоги щодо внесення до таких сертифікатів об’єктного ідентифікатора (OID) політики сертифіката, визначеного Мінцифри в межах реалізації вимог стандартів, у тому числі щодо забезпечення сумісності.

Звіт про оцінку відповідності видається за результатами процедури оцінки відповідності, проведеної відповідно до пункту 1 статті 20 зазначеного Регламенту.

114. Центральний засвідчувальний орган відповідно до частини першої статті 7 Закону України “Про електронну ідентифікацію та електронні довірчі послуги” здійснює аналіз звіту про оцінку відповідності, виданого органом з оцінки відповідності за результатами проведення процедури оцінки відповідності, зокрема отриманого разом з поданням засвідчувального центру.

115. Інформація, що подається кваліфікованим надавачем довірчих послуг або особою, яка має намір надавати кваліфіковані електронні довірчі послуги, для внесення відомостей до файлу Довірчого списку TL-UA-EC, повинна містити такі відомості та документи:

1) для юридичних осіб − повне найменування юридичної особи згідно з Єдиним державним реєстром юридичних осіб, фізичних осіб − підприємців та громадських формувань, код за ЄДРПОУ, країна, в якій зареєстрована юридична особа, прізвище, власне ім'я, по батькові (за наявності) керівника юридичної особи або його уповноваженого представника, серія (за наявності) і номер паспорта, ким і коли виданий;

2) для фізичних осіб − підприємців − прізвище, власне ім'я, по батькові (за наявності), реєстраційний номер облікової картки платника податків або серія (за наявності) та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган та мають відмітку в паспорті);

3) контактна інформація (номер телефону, електронна адреса інформаційного ресурсу, адреса електронної пошти, поштова адреса);

4) уніфіковані ідентифікатори ресурсів (URI), що забезпечують прямий доступ до актуальних версій таких документів: регламенту роботи кваліфікованого надавача довірчих послуг (політика сертифіката, положення сертифікаційних практик) та інших документів, що визначають правила і процедури надання кваліфікованих електронних довірчих послуг, про які повідомляється;

5) оцінку ризиків і наслідків відповідно до розділу 7 ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) "Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки";

6) перелік кваліфікованих електронних довірчих послуг, які надає або має намір надавати кваліфікований надавач довірчих послуг або особа, що має намір надавати кваліфіковані електронні довірчі послуги, та відомості про які пропонується внести до файлу Довірчого списку TL-UA-EC;

7) щодо кожної кваліфікованої електронної довірчої послуги, яку надає або має намір надавати кваліфікований надавач довірчих послуг або особа, що має намір надавати кваліфіковані електронні довірчі послуги:

один або декілька ідентифікаторів (ідентифікатори типів кваліфікованих електронних довірчих послуг, об'єктні ідентифікатори);

дату початку надання кваліфікованої електронної довірчої послуги або, якщо надання такої послуги не розпочато, заплановану дату початку її надання;

звіт про оцінку відповідності, зазначений у пункті 112 цих вимог, а також контактні дані органу з оцінки відповідності, який видав такий звіт;

технічні звіти, що підтверджують звіт про оцінку відповідності (за наявності), зокрема протоколи випробувань засобів кваліфікованого електронного підпису чи печатки на відповідність державним або міжнародним

стандартам, звіти про результати тестування на вразливість та відповідність ідентифікаторів у сертифікатах технічним специфікаціям;

підтвердження надсилання контролюючому органу копії документа про відповідність відповідно до частини дев'ятої статті 32 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”, разом із копіями оцінки ризиків і наслідків та технічних звітів, передбачених цими вимогами;

8) план припинення діяльності з надання кваліфікованих електронних довірчих послуг згідно з формою, затвердженою Мінцифри.

116. Центральний засвідчувальний орган з метою визначення відповідності кваліфікованого надавача довірчих послуг або особи, яка має намір надавати кваліфіковані електронні довірчі послуги, а також відповідних кваліфікованих електронних довірчих послуг Вимогам ЄС та вимогам законодавства у сферах електронної ідентифікації та електронних довірчих послуг, здійснює аналіз поданої інформації та доданих до неї документів, а саме оцінює:

1) підтвердження відповідності Вимогам ЄС кваліфікованого надавача довірчих послуг або особи, яка має намір надавати кваліфіковані електронні довірчі послуги, а також відповідних кваліфікованих електронних довірчих послуг, про що зазначено у звіті про оцінку відповідності;

2) відповідність звіту про оцінку відповідності вимогам, викладеним у нормативно-правових актах, прийнятих на виконання законодавства у сферах електронної ідентифікації та електронних довірчих послуг;

3) наявність у звіті про оцінку відповідності відомостей, що свідчать про невідповідність вимогам законодавства у сферах електронної ідентифікації та електронних довірчих послуг;

4) будь-які додаткові відомості, які необхідні для перевірки відповідності вимогам законодавства у сферах електронної ідентифікації та електронних довірчих послуг.

Для забезпечення повноти перевірки центральний засвідчувальний орган може здійснювати таку оцінку кваліфікованого надавача довірчих послуг або особи, яка має намір надавати кваліфіковані електронні довірчі послуги, за її місцезнаходженням, а також проводити співбесіди з представниками кваліфікованого надавача довірчих послуг або особи, яка має намір надавати кваліфіковані електронні довірчі послуги, та органу з оцінки відповідності.

117. Звіт про оцінку відповідності, інформація та документи, визначені пунктами 112 і 115 цих вимог, подаються кваліфікованим надавачем довірчих послуг або особою, яка має намір надавати кваліфіковані електронні довірчі послуги, в електронній формі до центрального засвідчувального органу через програмний інтерфейс інформаційно-комунікаційної системи центрального засвідчувального органу або електронну пошту технічного адміністратора

інформаційно-комунікаційної системи центрального засвідчувального органу support.its@czo.gov.ua, а до засвідчувального центру − на адресу електронної пошти Національного банку або через систему електронної взаємодії органів виконавчої влади чи систему електронної пошти Національного банку. Зазначені звіт про оцінку відповідності, інформація та документи повинні бути підписані шляхом накладення кваліфікованого електронного підпису керівника відповідної юридичної особи, фізичної особи − підприємця або їх уповноваженого представника.

Засвідчувальний центр не пізніше одного робочого дня з дати отримання зазначених звіту про оцінку відповідності, інформації та документів надсилає їх центральному засвідчувальному органу разом із поданням.

118. Центральний засвідчувальний орган розглядає подані звіт про оцінку відповідності, інформацію та документи протягом строку, що не перевищує трьох місяців з дати їх отримання. Якщо розгляд не завершено протягом трьох місяців з дати отримання такої інформації, центральний засвідчувальний орган інформує особу, яка подала зазначені звіт про оцінку відповідності, інформацію та документи, із зазначенням причин затримки та строку, у межах якого має бути завершено розгляд.

119. Перевірка відповідності кваліфікованого надавача довірчих послуг або особи, яка має намір надавати кваліфіковані електронні довірчі послуги, а також відповідних кваліфікованих електронних довірчих послуг Вимогам ЄС здійснюється шляхом взаємодії з контролюючим органом у межах загального строку розгляду за такою процедурою:

1) центральний засвідчувальний орган не пізніше одного робочого дня з дати реєстрації звіту про оцінку відповідності, інформації та документів, визначених пунктами 112 і 115 цих вимог, надсилає контролюючому органу в електронній формі запит разом із зазначеними звітом про оцінку відповідності, інформацією та документами щодо підтвердження відповідності такого кваліфікованого надавача довірчих послуг або особи, яка має намір надавати кваліфіковані електронні довірчі послуги, а також відповідних кваліфікованих електронних довірчих послуг Вимогам ЄС;

2) контролюючий орган здійснює відповідні заходи нагляду (контролю) та надає інформацію про їх результати центральному засвідчувальному органу без необґрунтованої затримки, у будь-якому разі не пізніше ніж через два місяці з дати отримання запиту. Якщо перевірку не завершено контролюючим органом протягом двох місяців із дати отримання запиту, контролюючий орган інформує центральний засвідчувальний орган із зазначенням причин затримки та строку, протягом якого буде завершено перевірку;

3) за результатами розгляду та перевірки контролюючий орган надає центральному засвідчувальному органу офіційну відповідь про відповідність кваліфікованого надавача довірчих послуг або особи, яка має намір надавати кваліфіковані електронні довірчі послуги, а також відповідних кваліфікованих

електронних довірчих послуг Вимогам ЄС або про виявлені невідповідності таким вимогам.

120. Центральний засвідчувальний орган у строк, визначений пунктом 118 цих вимог, на підставі поданих звіту про оцінку відповідності, інформації та документів, визначених пунктами 112 і 115 цих вимог, а також офіційної відповіді контролюючого органу приймає одне з таких рішень:

1) про внесення до файлу Довірчого списку TL-UA-EC відомостей про кваліфікованого надавача довірчих послуг або особу, яка має намір надавати кваліфіковані електронні довірчі послуги, та відповідні кваліфіковані електронні довірчі послуги або про окрему кваліфіковану електронну довірчу послугу, відомості про яку відсутні у такому файлі;

2) про відмову у внесенні відомостей до файлу Довірчого списку TL-UA-EC.

Центральний засвідчувальний орган повідомляє про прийняте рішення кваліфікованого надавача довірчих послуг або особу, яка має намір надавати кваліфіковані електронні довірчі послуги, та/або засвідчувальний центр шляхом надсилання копії такого рішення.

121. Адміністратор інформаційно-комунікаційної системи центрального засвідчувального органу розміщує на офіційному вебсайті центрального засвідчувального органу та підтримує в актуальному стані таку інформацію:

1) контактну інформацію Мінцифри:

місцезнаходження (поштова адреса);

телефон, адреса електронної пошти та вебсайту;

2) щодо порядку та способу подання інформації та документів, необхідних для отримання адміністративної послуги із внесення відомостей про юридичних осіб та фізичних осіб − підприємців, які мають намір надавати кваліфіковані електронні довірчі послуги, до файлу Довірчого списку TL-UA-EC;

3) вичерпний перелік документів, необхідних для отримання адміністративної послуги із внесення відомостей про юридичних осіб та фізичних осіб - підприємців, які мають намір надавати кваліфіковані електронні довірчі послуги, до файлу Довірчого списку TL-UA-EC;

4) про те, що рішення про відмову у внесенні відомостей про юридичних осіб та фізичних осіб − підприємців, які мають намір надавати кваліфіковані електронні довірчі послуги, до файлу Довірчого списку TL-UA-EC може бути оскаржене в суді в порядку адміністративного судочинства;

5) загальний опис процедури перевірки відповідності кваліфікованих надавачів довірчих послуг або осіб, які мають намір надавати кваліфіковані електронні довірчі послуги, а також відповідних кваліфікованих електронних довірчих послуг Вимогам ЄС.”;

19) У Переліку стандартів, що застосовуються кваліфікованими надавачами електронних довірчих послуг для надання кваліфікованих електронних довірчих послуг, що додається до вимог до надавачів послуг електронної ідентифікації та електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 28 червня 2024 р. № 764 (Офіційний вісник України, 2024 р., № 63, ст. 3762):

пункт 2 викласти в такій редакції:

“2. ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”.”;

пункт 4 викласти в такій редакції:

“4. ДСТУ ETSI TS 119 403-2:2026 (ETSI TS 119 403-2 V1.3.1 (2023-03), IDT) “Електронні підписи та інфраструктури (ESI). Оцінювання відповідності надавачів довірчих послуг. Частина 2. Додаткові вимоги до органів оцінювання відповідності, що перевіряють постачальників довірчих послуг, які видають довірчі сертифікати”.”;

пункти 6, 7 викласти в такій редакції:

“6. ДСТУ ETSI TS 119 441:2026 (ETSI TS 119 441 V1.2.1 (2023-10), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики стосовно TSP, що надає послуги щодо перевіряння підписів”.”;

7. ДСТУ ETSI TS 119 461:2026 (ETSI TS 119 461 V2.1.1 (2025-02), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для компонентів довірчих послуг, що забезпечують перевіряння особи суб'єктів довірчих послуг”.”;

пункт 11 викласти в такій редакції:

“11. ДСТУ ETSI TS 119 612:2026 (ETSI TS 119 612 V2.4.1 (2025-08), IDT) “Електронні підписи та інфраструктури (ESI). Довірчі списки”.”;

пункт 13 викласти в такій редакції:

“13. ДСТУ ETSI TS 119 615:2026 (ETSI TS 119 615 V1.2.1 (2023-06), IDT) “Електронні підписи та інфраструктури (ESI). Довірчі списки. Процедури використання та тлумачення національних довірчих списків держав-членів Європейського Союзу”.”;

пункти 18, 19 викласти в такій редакції:

“18. ДСТУ ETSI EN 319 102-1:2026 (ETSI EN 319 102-1 V1.4.1 (2024-06), IDT) “Електронні підписи та інфраструктури (ESI). Процедури створення та перевіряння цифрових підписів AdES. Частина 1. Створення та перевіряння”.

19. ДСТУ ETSI TS 119 102-2:2026 (ETSI TS 119 102-2 V1.4.1 (2023-06), IDT) “Електронні підписи та інфраструктури (ESI). Процедури створення та

перевіряння цифрових підписів AdES. Частина 2. Звіт про перевіряння підпису”.”;

пункт 24 викласти в такій редакції:

“24. ДСТУ ETSI TS 119 441:2026 (ETSI TS 119 441 V1.2.1 (2023-10), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики стосовно TSP, що надає послуги щодо перевіряння підписів”.”;

пункт 26 викласти в такій редакції:

“26. ДСТУ ETSI EN 319 122-1:2026 (ETSI EN 319 122-1 V1.3.1 (2023-06), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Частина 1. Структурні блоки та базові підписи CAdES”.”;

пункт 28 виключити;

пункт 30 викласти в такій редакції:

“30. ДСТУ ETSI EN 319 142-1:2026 (ETSI EN 319 142-1 V1.2.1 (2024-01), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Частина 1. Структурні блоки та базові підписи PAdES”.”;

пункт 35 викласти в такій редакції:

“35. ДСТУ ETSI TS 119 182-1:2026 (ETSI TS 119 182-1 V1.2.1 (2024-07), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи JAdES. Частина 1. Структурні блоки та базові підписи JAdES”.”;

після пункту 35 доповнити новими пунктами 35^1-35^4 такого змісту:

“35^1. ДСТУ ETSI TS 103 171:2018 (ETSI TS 103 171:2012, IDT) “Електронні підписи та інфраструктури (ESI). Базовий профіль XAdES”.

35^2. ДСТУ ETSI TS 103 172:2018 (ETSI TS 103 172:2013, IDT) “Електронні підписи та інфраструктури (ESI). Базовий профіль PAdES”.

35^3. ДСТУ ETSI TS 103 173:2018 (ETSI TS 103 173:2013, IDT) “Електронні підписи та інфраструктури (ESI). Базовий профіль CAdES”.

35^4. ДСТУ ETSI TS 103 174:2018 (ETSI TS 103 174:2013, IDT) “Електронні підписи та інфраструктури (ESI). Базовий профіль ASiC”.;

пункти 42, 43 викласти в такій редакції:

“42. ДСТУ ETSI EN 319 411-1:2026 (ETSI EN 319 411-1 V1.5.1 (2025-04), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги”.

43. ДСТУ ETSI EN 319 411-2:2026 (ETSI EN 319 411-2 V2.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2.

Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС”.[1]”;

пункт 46 викласти в такій редакції:

“46. ДСТУ ETSI EN 319 421:2026 (ETSI EN 319 421 V1.3.1 (2025-07), IDT) “Електронні підписи та інфраструктури (ESI). Політика та вимоги безпеки щодо надавачів довірчих послуг, які видають часові штемпелі”.”;

пункт 60 викласти в такій редакції:

“60. ДСТУ ETSI TS 119 431-1:2026 (ETSI TS 119 431-1 V1.3.1 (2024-12), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг. Частина 1. Послуги TSP, що працюють з віддаленим QSCD/SCDev”.”;

пункт 63 викласти в такій редакції:

“63. ДСТУ ETSI TS 119 495:2026 (ETSI TS 119 495 V1.8.1 (2026-04), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги до специфічних секторів. Профілі сертифікатів та вимоги щодо політики TSP для відкритого банкінгу”.”;

пункти 65 − 67 викласти в такій редакції:

“65. ДСТУ ETSI EN 319 412-1:2026 (ETSI EN 319 412-1 V1.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та загальні структури даних”.

66. ДСТУ ETSI EN 319 412-2:2026 (ETSI EN 319 412-2 V2.4.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 2. Профіль сертифіката для сертифікатів, виданих фізичним особам”.

67. ДСТУ ETSI EN 319 412-3:2026 (ETSI EN 319 412-3 V1.3.1 (2023-09), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 3. Профіль сертифіката для сертифікатів, виданих юридичним особам”.”;

пункт 69 викласти в такій редакції:

“69. ДСТУ ETSI EN 319 412-5:2026 (ETSI EN 319 412-5 V2.5.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 5. Заяви про якість”.”;

20) доповнити новим розділом такого змісту:

“Стандарти щодо отримання та використання гаманців з цифровою ідентифікацією

121. ДСТУ ISO/IEC 18013-5:2026 (ISO/IEC 18013-5:2021, IDT) “Ідентифікація особи. Водійське посвідчення, що відповідає стандартам ISO. Частина 5. Застосунок щодо користування мобільним водійським посвідченням (mDL)”.

122. ДСТУ ISO/IEC TS 18013-7:2026 (ISO/IEC TS 18013-7:2025, IDT) “Ідентифікація особи. Водійське посвідчення, що відповідає стандартам ISO. Частина 7. Додаткові функції мобільного водійського посвідчення (mDL)”.

123. ДСТУ ETSI TS 119 471:2026 (ETSI TS 119 471 V1.1.1 (2025-05), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників послуг електронної сертифікації атрибутів”.

21) доповнити новою приміткою такого змісту:

Примітка 1. У стандарті ДСТУ ETSI EN 319 411-2:2026 (ETSI EN 319 411-2 V2.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС” вимоги Регламенту (ЄС) № 910/2014 Європейського Парламенту і Ради від 23 липня 2014 р. про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС забезпечуються шляхом виконання норм Закону України "Про електронну ідентифікацію та електронні довірчі послуги" та інших нормативно-правових актів у сферах електронної ідентифікації та електронних довірчих послуг.”.

2. Абзац другий пункту 9 Порядку використання псевдонімів фізичними особами, які є користувачами послуг електронної ідентифікації або електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 28 червня 2024 р. № 764 (Офіційний вісник України, 2024 р., № 63, ст. 3762; 2026 р.) викласти в такій редакції:

“При цьому надавачі довірчих послуг повинні враховувати положення ДСТУ ETSI EN 319 412-2:2026 (ETSI EN 319 412-2 V2.4.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 2. Профіль сертифіката для сертифікатів, виданих фізичним особам”.”.

3. У Положенні про інтегровану систему електронної ідентифікації, затвердженому постановою Кабінету Міністрів України від 3 листопада 2023 р. № 1150 (Офіційний вісник України, 2023 р., № 101, ст. 6026; 2025 р., № 91, ст. 6365; 2026 р., № 9, ст. 746):

1) у пункті 2:

абзаци шостий − тринадцятий замінити абзацами такого змісту:

“прикладний програмний інтерфейс − інтерфейс програмування, призначений для підключення інформаційно-комунікаційних систем суб’єктів взаємодії до системи;

програмний інтерфейс − набір визначених підпрограм та протоколів обміну інформацією для взаємодії різних програмних компонентів;

проміжні вузли електронної ідентифікації (хаби) − об’єкти інфраструктури послуг з електронної ідентифікації та їх інформаційно-комунікаційні системи, які створюються кваліфікованими надавачами електронних довірчих послуг та іншими суб’єктами для схем електронної ідентифікації;

протокол визначення статусу сертифіката − протокол обміну інформацією під час інтерактивного визначення статусу сертифіката відкритого ключа за запитами користувачів системи;

протокол обміну інформацією − перелік форматів переданих блоків даних, набір правил їх обробки і правил взаємодії інформаційно-комунікаційних систем на одному рівні;

протокол управління сертифікатом − протокол обміну інформацією під час отримання сертифіката та відомостей про його статус за запитами користувачів системи;

реєстраційний сертифікат довіряючої сторони − об’єкт даних, що містить відомості про мету використання гаманця з цифровою ідентифікацією довіряючою стороною та перелік атрибутів, які така сторона має право запитувати у користувачів, виданий адміністратором системи;

сертифікат доступу довіряючої сторони − сертифікат електронного підпису чи печатки, що використовується для автентифікації довіряючої сторони та валідації даних про неї під час взаємодії довіряючої сторони з гаманцем з цифровою ідентифікацією, виданий адміністратором системи;

транскордонна електронна ідентифікація − електронна ідентифікація користувачів системи з використанням засобів електронної ідентифікації, виданих у межах схеми електронної ідентифікації іншої держави.”;

2) абзац шістнадцятий викласти в такій редакції:

“Інші терміни у цьому Положенні вживаються у значенні, наведеному в Законах України “Про інформацію”, “Про Національну програму інформатизації”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про електронні комунікації”, “Про захист персональних даних”, “Про електронну ідентифікацію та електронні довірчі послуги”, “Про основні засади забезпечення кібербезпеки України”, “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус”, “Про публічні електронні реєстри”, вимогах до випуску гаманців з цифровою ідентифікацією, затверджених постановою Кабінету Міністрів України від 11 червня 2025 р. № 689 (Офіційний вісник України, 2025 р., № 54, ст. 3760) та інших нормативно-правових актах у сферах електронної ідентифікації та електронних довірчих послуг.”;

3) у пункті 15:

абзац чотирнадцятий викласти в такій редакції:

“електронну інформаційну взаємодію з кваліфікованими надавачами електронних довірчих послуг з метою валідації атрибутів, зазначених в електронних посвідченнях атрибутів, відповідно до переліку, визначеного у додатку до цього Положення, шляхом перевірки інформації з відомостями публічних електронних реєстрів на запит такого кваліфікованого надавача в інтересах фізичної або юридичної особи, якій належать відповідні атрибути;”;

доповнити новими абзацами такого змісту:

“видачу, оновлення, зупинення дії та скасування сертифікатів доступу довіряючої сторони для взаємодії довіряючої сторони з гаманцями з цифровою ідентифікацією;

видачу, оновлення, зупинення дії та скасування реєстраційних сертифікатів довіряючої сторони для взаємодії довіряючої сторони з гаманцями з цифровою ідентифікацією;

публікацію інформації про статус сертифікатів доступу довіряючої сторони та реєстраційних сертифікатів довіряючої сторони відповідно до вимог до випуску гаманців з цифровою ідентифікацією, затверджених постановою Кабінету Міністрів України від 11 червня 2025 р. № 689 та інших актів законодавства;”;

4) назву додатка до Положення викласти в такій редакції:

“**ПЕРЕЛІК**
атрибутів фізичних та юридичних осіб, щодо яких здійснюється валідація з використанням відомостей, що містяться в публічних електронних реєстрах”.

4. У постанові Кабінету Міністрів України від 13 вересня 2024 р. № 1062 “Про затвердження Порядку проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг” (Офіційний вісник України, 2024 р., № 86, ст. 5358):

1) назву постанови викласти в такій редакції:

“Деякі питання акредитації органів з оцінки відповідності та проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг”;

2) пункт 1 викласти в такій редакції:

“Затвердити такі, що додаються:

Порядок проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг;

Порядок проведення процедури акредитації органів з оцінки відповідності, які здійснюють оцінку відповідності кваліфікованих надавачів електронних

довірчих послуг та кваліфікованих електронних довірчих послуг, що ними надаються.”;

3) у Порядку проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг, затвердженому зазначеною постановою:

пункт 3 викласти в такій редакції:

“3. У цьому Порядку терміни вживаються у такому значенні:

замовник процедури оцінки відповідності (далі − замовник) − юридична особа, фізична особа − підприємець, яка має намір надавати послуги електронної ідентифікації, надавач послуг електронної ідентифікації, а також юридична особа, фізична особа − підприємець, яка має намір надавати кваліфіковані електронні довірчі послуги, кваліфікований надавач електронних довірчих послуг, центральний засвідчувальний орган, засвідчувальний центр;

звіт про оцінку відповідності – документ, що складається органом з оцінки відповідності за результатами проведення процедури оцінки відповідності та містить детальну інформацію про метод проведення оцінки відповідності відповідного об’єкта оцінки відповідності, застосовну схему оцінки відповідності, вимоги законодавства у сферах електронної ідентифікації та електронних довірчих послуг, національні стандарти та/або технічні специфікації, щодо відповідності яким проводилася така оцінка, а також про результати такої оцінки;

об’єкт оцінки відповідності − юридична особа, фізична особа − підприємець, яка має намір надавати кваліфіковані електронні довірчі послуги, послуги електронної ідентифікації, надавач послуг електронної ідентифікації, кваліфікований надавач електронних довірчих послуг, центральний засвідчувальний орган або засвідчувальний центр та послуги, які вони надають, засоби кваліфікованого електронного підпису чи печатки, які використовуються або використовуватимуться під час надання кваліфікованих електронних довірчих послуг;

Інші терміни в цьому Порядку вживаються у значенні, наведеному в Законах України “Про електронну ідентифікацію та електронні довірчі послуги”, “Про захист інформації в інформаційно-комунікаційних системах” та прийнятих відповідно до них нормативно-правових актах.”;

у пункті 6 слова “аудиторський звіт”, “Аудиторський звіт” замінити відповідно словами “звіт про оцінку відповідності”, “Звіт про оцінку відповідності”;

абзац другий пункту 7 викласти в такій редакції:

“Органи з оцінки відповідності під час проведення оцінки відповідності у сфері електронних довірчих послуг повинні дотримуватися положень, визначених у стандартах ДСТУ ETSI EN 319 403-1:2021 (ETSI EN 319 403-1

V2.3.1 (2020-06), IDT) “Електронні підписи та інфраструктури (ESI). Оцінювання відповідності постачальників довірчих послуг. Частина 1. Вимоги до органів оцінювання відповідності, які оцінюють постачальників довірчих послуг”, ДСТУ ETSI TS 119 403-2:2026 (ETSI TS 119 403-2 V1.3.1 (2023-03), IDT) “Електронні підписи та інфраструктури (ESI). Оцінювання відповідності надавачів довірчих послуг. Частина 2. Додаткові вимоги до органів оцінювання відповідності, що перевіряють постачальників довірчих послуг, які видають довірчі сертифікати”, ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”.”;

пункти 8 і 9 виключити;

пункти 10-16 викласти в такій редакції:

“10. Оцінка відповідності проводиться двома етапами:

перший етап передбачає проведення оцінки документації, в тому числі планування другого етапу шляхом визначення структури та обсягу послуг, що надаватиме замовник;

другий етап передбачає виїзний захід за місцезнаходженням замовника, завершення оцінювання послуг та погодження органом з оцінки відповідності плану коригувальних дій замовника (у разі подання замовником плану коригувальних дій відповідно до пункту 13 цього Порядку).

За результатами кожного етапу оцінки відповідності складається звіт за результатами відповідного етапу. Під час встановлення інтервалу між першим та другим етапами оцінки відповідності необхідно враховувати обсяги перевірки та потреби замовника для вирішення проблемних питань, виявлених під час проведення першого етапу, з урахуванням строку, передбаченого абзацом шостим цього пункту.

Орган з оцінки відповідності після завершення другого етапу оцінки відповідності повинен у письмовій формі у передбачений у договорі спосіб поінформувати замовника про всі невідповідності та інші висновки, зазначені у звіті про оцінку відповідності, із зазначенням їх суттєвого впливу на безпеку та/або здатність надавати кваліфіковані електронні довірчі послуги чи послуги електронної ідентифікації.

За результатами проведення оцінки відповідності орган з оцінки відповідності у строк, що не може бути більшим ніж шість місяців з дати укладення договору, складає та видає замовнику звіт про оцінку відповідності.

11. За результатами проведення оцінки відповідності органом з оцінки відповідності приймається одне з таких рішень, яке відображається у звіті про оцінку відповідності:

1) про відповідність об’єкта оцінки відповідності вимогам у повному обсязі;

2) про невідповідність об’єкта оцінки відповідності вимогам.

12. У разі прийняття рішення про відповідність об’єкта оцінки відповідності вимогам орган з оцінки відповідності видає замовнику звіт про оцінку відповідності з висновком про відповідність.

13. У разі прийняття рішення про невідповідність об’єкта оцінки відповідності вимогам орган з оцінки відповідності видає замовнику звіт про оцінку відповідності з висновком про невідповідність об’єкта оцінки відповідності вимогам (далі − висновок про невідповідність) із зазначенням недоліків.

Після усунення невідповідностей, зазначених у звіті про оцінку відповідності, замовник на умовах та в строки, визначені в договорі, може продовжити процедуру оцінки відповідності відповідно до пункту 13 цього Порядку або пройти процедуру оцінки відповідності повторно.

14. Звіт про оцінку відповідності, складений за результатами процедури оцінки відповідності, передбаченої частиною першою статті 32 Закону, повинен відповідати таким вимогам:

1) звіт має супроводжуватися рішенням про сертифікацію відповідно до пункту 7.6 стандарту ДСТУ ETSI EN 319 403-1:2021 (ETSI EN 319 403-1 V2.3.1 (2020-06), IDT) “Електронні підписи та інфраструктури (ESI). Оцінювання відповідності постачальників довірчих послуг. Частина 1. Вимоги до органів оцінювання відповідності, які оцінюють постачальників довірчих послуг”, яке підтверджує, чи особа, щодо якої проведено оцінку відповідності, та кваліфіковані електронні довірчі послуги, що нею надаються або мають надаватися, відповідають вимогам законодавства у сферах електронної ідентифікації та електронних довірчих послуг, застосовних стандартів та відповідної схеми оцінки відповідності;

2) звіт має містити інформацію про особу, щодо якої проведено оцінку відповідності:

для юридичної особи: найменування, код згідно з ЄДРПОУ, відомості про місцезнаходження юридичної особи та електронну адресу, а також, за наявності, такі самі відомості для всіх дочірніх, афілійованих юридичних осіб, підрядників та субпідрядників, що беруть участь у наданні кваліфікованих електронних довірчих послуг;

для фізичної особи − підприємця: прізвище, власне ім’я, по батькові (за наявності), унікальний номер запису в Єдиному державному демографічному реєстрі або відомості про реєстраційний номер облікової картки платника податків або номер паспорта громадянина України (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та офіційно повідомили про це відповідний податковий орган і мають відмітку або інформацію в паспорті громадянина України про право здійснювати будь-які платежі за серією та/або номером

паспорта), або номер паспортного документа іноземця чи особи без громадянства), місце проживання (перебування) та електронну адресу;

3) звіт має включати детальний опис сфери проведеної оцінки відповідності, включаючи конкретні кваліфіковані електронні довірчі послуги, охоплені такою оцінкою;

4) звіт має містити достатні докази, що підтверджують відповідність особи, щодо якої проведено оцінку відповідності, та кваліфікованих електронних довірчих послуг, що нею надаються або мають надаватися, вимогам законодавства у сферах електронної ідентифікації та електронних довірчих послуг, застосовних стандартів та відповідної схеми оцінки відповідності;

5) звіт має містити найменування органу з оцінки відповідності, код згідно з ЄДРПОУ або інший реєстраційний номер відповідно до законодавства держави його місцезнаходження, відомості про його місцезнаходження та електронну адресу;

6) містити такі відомості:

найменування національного органу з акредитації, який акредитував орган з оцінки відповідності;

прізвища, імена та по батькові (за наявності) осіб, залучених органом з оцінки відповідності до проведення оцінки відповідності, та їхню роль у такій оцінці;

посилання на сторінку офіційного вебсайту національного органу з акредитації, що акредитував орган з оцінки відповідності, на якій опубліковано атестат про акредитацію органу з оцінки відповідності;

цифровий символ акредитації (за наявності);

схему оцінки відповідності, для якої орган з оцінки відповідності був акредитований відповідно до пункту 3 цього Порядку;

перевірки оцінки відповідності, обґрунтування їх вибору та застосовану методологію, включаючи методологію вибірки та процедури випробувань;

відповідну схему оцінки відповідності та відповідні документи або посилання на місце, де така схема та відповідні документи доступні;

7) містити щонайменше один кваліфікований електронний підпис, якщо звіт подається в електронній формі, або власноручний підпис, якщо звіт подається в паперовій формі, із зазначенням прізвища, імені та по батькові (за наявності) та посади відповідальної особи (осіб), уповноваженої(их) ухвалювати рішення про сертифікацію від імені органу з оцінки відповідності;

8) стосуватися однієї юридичної особи або фізичної особи — підприємця, щодо якої проведено оцінку відповідності;

9) ідентифікувати, відповідно до підпункту 5.5.3 пункту 5.5 розділу 5 ДСТУ ETSI TS 119 612:2026 (ETSI TS 119 612 V2.4.1 (2025-08), IDT) “Електронні підписи та інфраструктури (ESI). Довірчі списки”, цифрові ідентифікатори послуг за типом кваліфікованої електронної довірчої послуги, для якої підтверджується відповідність вимогам Закону, із наданням такої інформації:

якщо кваліфікована електронна довірча послуга не базується на технології інфраструктури відкритих ключів − ідентифікатор у формі URI, що однозначно ідентифікує кваліфіковану електронну довірчу послугу;

якщо кваліфікована електронна довірча послуга базується на технології інфраструктури відкритих ключів − щонайменше таке: ідентифікатор ключа суб’єкта (Subject Key Identifier) відповідно до IETF RFC 5280 “Профіль сертифікатів та списків відкликання сертифікатів (CRL) інфраструктури відкритих ключів X.509 для мережі Інтернет”; представлення у форматі Base64 PEM відповідного цифрового сертифіката X.509v3; у відповідних випадках, зазначення того, чи конкретні набори або піднабори сертифікатів кінцевих суб’єктів, виданих на підставі або під егідою цифрового ідентифікатора послуги, виключені з рішення про сертифікацію або спеціально включені до нього, та на підставі яких критеріїв вони можуть бути ідентифіковані; зазначення того, чи цифровий ідентифікатор послуги стосується кінцевого суб’єкта або кваліфікованого надавача електронних довірчих послуг; опис того, як цифровий ідентифікатор послуги використовується в контексті відповідної кваліфікованої електронної довірчої послуги;

10) містити, у відповідних випадках, детальний опис функціональної ієрархії інфраструктури відкритих ключів, за типом кваліфікованої електронної довірчої послуги та для всіх цифрових ідентифікаторів послуг, ідентифікованих відповідно до підпункту 9 цього пункту;

11) містити вичерпний перелік третіх осіб, включаючи субпідрядників, які забезпечують компоненти кваліфікованих електронних довірчих послуг, із зазначенням їхнього найменування та місцезнаходження, а також зазначення того, чи ці треті особи та їхні об’єкти були предметом оцінки відповідності та в якому обсязі;

12) описувати, у відповідних випадках, зміст запису, що підлягає включенню або оновленню у відповідному Довірчому списку відповідно до результатів оцінки відповідності;

13) містити вичерпний перелік публічних та внутрішніх документів особи, щодо якої проведено оцінку відповідності, із належною ідентифікацією, включаючи версіонування, зокрема:

регламент роботи кваліфікованого надавача електронних довірчих послуг (політика сертифіката, положення сертифікаційних практик та інші документи, що визначають правила і процедури надання електронних довірчих послуг);

умови договорів із підписувачами;

план припинення діяльності з надання кваліфікованих електронних довірчих послуг;

документацію, пов’язану з оцінкою ризиків;

план повідомлення про порушення безпеки;

перелік усіх внутрішніх документів, що забезпечують ефективне впровадження практик кваліфікованого надавача електронних довірчих послуг;

установчі документи особи, щодо якої проведено оцінку відповідності, а також організаційну структуру, інформацію про структуру власності та, у відповідних випадках, звіт аудитора за попередні два звітних роки;

відомості або документи, що підтверджують наявність фінансового забезпечення (коштів на рахунку із спеціальним режимом використання) для забезпечення відшкодування шкоди, яка може бути завдана користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання кваліфікованим надавачем електронних довірчих послуг своїх зобов’язань або страхування відповідальності для забезпечення відшкодування такої шкоди;

перелік стандартів, відповідність яким заявлена;

перелік стандартів, відповідність яким підтверджена аудитом, оцінкою відповідності або сертифікацією;

перелік засобів кваліфікованого електронного підпису чи печатки та інформацію про їхню сертифікацію, якщо кваліфікований надавач електронних довірчих послуг надає або забезпечує доступність таких засобів;

перелік пристроїв, що використовуються як надійні системи або продукти для захисту ключів, та інформацію про їхню сертифікацію;

14) містити оцінку виконання вимог, що застосовуються до відповідних кваліфікованих електронних довірчих послуг, перелік яких визначено в частині третій статті 16 Закону;

15) містити оцінку виконання вимог, що застосовуються до особи, щодо якої проведено оцінку відповідності, та відповідних кваліфікованих електронних довірчих послуг відповідно до законодавства у сферах кібербезпеки та захисту інформації;

16) містити заяву, що декларує, у відповідних випадках, відсутність будь-яких невідповідностей; у разі виявлення невідповідностей − звіт повинен містити план коригувальних дій із графіком їх виконання, наданий особою, щодо якої проведено оцінку відповідності, та погоджений органом з оцінки відповідності, разом з описом запланованих заходів оцінки для підтвердження усунення таких невідповідностей;

17) містити, у відповідних випадках, зазначення можливостей для покращення щодо виконання особою, щодо якої проведено оцінку відповідності, відповідних вимог;

18) ідентифікувати для кожного етапу оцінки відповідності, включаючи аудит документації, оцінку впровадження та виїзне оцінювання, період, за який проводилась оцінка відповідності, та час, витрачений органом з оцінки відповідності в людино-днях;

19) ідентифікувати у відповідному звіті щодо конкретних вимог детальні перевірки оцінки відповідності та цілі перевірки, що проводилися під час такої оцінки, або містити посилання на окремі звіти з оцінки, за умови що такі окремі звіти видані акредитованими органами з оцінки відповідності та підтверджені органом з оцінки відповідності, що видає звіт про оцінку відповідності;

20) містити сферу, опис та результати значного набору випробувань або вибірок результатів надання оцінених кваліфікованих електронних довірчих послуг та їх оцінку для всіх відповідних і застосовних типів таких результатів;

21) зазначати такі строки:

строк, протягом якого повинно бути проведено наступне наглядове оцінювання відповідності;

строк, протягом якого повинна бути проведена наступна оцінка відповідності відповідно до частини першої статті 32 Закону;

22) містити заяву про те, що сертифікаційні документи, включаючи звіт про оцінку відповідності, також призначені для використання контролюючим органом.

Звіт про оцінку відповідності є частиною сертифікаційної документації, зазначеної в пункті 7.7 стандарту ДСТУ ETSI EN 319 403-1:2021 (ETSI EN 319 403-1 V2.3.1 (2020-06), IDT) “Електронні підписи та інфраструктури (ESI). Оцінювання відповідності постачальників довірчих послуг. Частина 1. Вимоги до органів оцінювання відповідності, які оцінюють постачальників довірчих послуг”.

15. Якщо за результатами оцінювання виявлено невідповідності та замовник має намір продовжити процедуру оцінки відповідності, він повинен у строк не більш як п’ять робочих днів з дати отримання відповідного звіту про оцінку відповідності подати органу з оцінки відповідності план коригувальних дій відповідно до стандарту ДСТУ ETSI EN 319 403-1:2021 у письмовій формі у спосіб, передбачений у договорі.

Орган з оцінки відповідності оцінює та погоджує план коригувальних дій, визначає строк їх проведення і завдання, які необхідно виконати для підтвердження того, що недоліки були виправлені, про що інформує замовника у письмовій формі у спосіб, передбачений у договорі.

16. У разі незначної невідповідності, а саме невиконання вимог, які не мають впливу на безпеку та здатність надавача послуг електронної ідентифікації чи кваліфікованого надавача електронних довірчих послуг надавати послуги електронної ідентифікації чи кваліфіковані електронні довірчі послуги, орган з оцінки відповідності повинен розглянути коригувальні дії, здійснені замовником, протягом:

трьох місяців з дати повідомлення замовника про невідповідності, виявлені під час оцінки відповідності;

шести місяців з дати повідомлення замовника про невідповідності, виявлені під час оцінки відповідності, − у разі подання замовником до органу з оцінки відповідності документального підтвердження, що проведення коригувальних дій потребує більш тривалого періоду у зв'язку із складністю їх виконання.";

4) доповнити постанову Порядком такого змісту:

"ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 13 вересня 2024 р. № 1062

ПОРЯДОК
проведення процедури акредитації органів з оцінки відповідності, які здійснюють оцінку відповідності кваліфікованих надавачів електронних довірчих послуг та кваліфікованих електронних довірчих послуг, що ними надаються

1. Цей Порядок визначає механізм та процедуру акредитації органів з оцінки відповідності, що здійснюють оцінку відповідності юридичних осіб та фізичних осіб − підприємців, які мають намір надавати кваліфіковані електронні довірчі послуги, кваліфікованих надавачів електронних довірчих послуг та кваліфікованих електронних довірчих послуг, що ними надаються або мають надаватися, вимоги до звіту про оцінку відповідності та схеми оцінки відповідності.

Цей Порядок застосовується для цілей експериментального проекту щодо взаємного визнання електронних довірчих послуг між Україною та Європейським Союзом, запровадженого згідно з постановою Кабінету Міністрів України від _____ № _____ "Деякі питання реалізації експериментального проекту щодо взаємного визнання електронних довірчих послуг між Україною та Європейським Союзом".

2. Для цілей цього Порядку терміни вживаються у такому значенні:

рішення про сертифікацію – рішення за результатами оцінки відповідності, проведеної органом з оцінки відповідності, яким такий орган підтверджує

відповідність або невідповідність конкретної юридичної особи або фізичної особи − підприємця, які мають намір надавати кваліфіковані електронні довірчі послуги, або кваліфікованого надавача електронних довірчих послуг та кваліфікованої електронної довірчої послуги, що такою особою або надавачем надається чи має надаватися, вимогам законодавства у сферах електронної ідентифікації та електронних довірчих послуг, застосовних стандартів та відповідної схеми оцінки відповідності;

сертифікат відповідності – документ, виданий органом з оцінки відповідності, що засвідчує позитивне рішення про сертифікацію щодо конкретної юридичної особи або фізичної особи — підприємця, які мають намір надавати кваліфіковані електронні довірчі послуги, або кваліфікованого надавача електронних довірчих послуг та кваліфікованої електронної довірчої послуги, що такою особою або надавачем надається чи має надаватися;

субпідрядник – юридична або фізична особа – підприємець, якій орган з оцінки відповідності доручає виконання окремих видів діяльності з оцінки відповідності;

схема оцінки відповідності – сукупність правил та процедур, що використовуються органами з оцінки відповідності для оцінки відповідності юридичних осіб та фізичних осіб – підприємців, які мають намір надавати кваліфіковані електронні довірчі послуги, кваліфікованих надавачів електронних довірчих послуг та кваліфікованих електронних довірчих послуг, що ними надаються або мають надаватися, вимогам законодавства у сферах електронної ідентифікації та електронних довірчих послуг та застосовним стандартам.

Інші терміни у цьому Порядку вживаються у значенні, наведеному в законах України “Про електронну ідентифікацію та електронні довірчі послуги”, “Про акредитацію органів з оцінки відповідності”, Порядку проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг, затвердженому постановою Кабінету Міністрів України від 13 вересня 2024 р. № 1062 (Офіційний вісник України, 2024 р., № 86, ст. 5358).

3. Органи з оцінки відповідності акредитуються для цілей прийняття рішень про сертифікацію відповідно до конкретної схеми оцінки відповідності згідно з ДСТУ EN ISO/IEC 17065:2019 (EN ISO/IEC 17065:2012, IDT; ISO/IEC 17065:2012, IDT) “Оцінка відповідності. Вимоги до органів з сертифікації продукції, процесів та послуг”, доповненим стандартом ДСТУ ETSI EN 319 403-1:2021 (ETSI EN 319 403-1 V2.3.1 (2020-06), IDT) “Електронні підписи та інфраструктури (ESI). Оцінювання відповідності постачальників довірчих послуг. Частина 1. Вимоги до органів оцінювання відповідності, які оцінюють постачальників довірчих послуг”.

4. Акредитація органів з оцінки відповідності, зазначена у пункті 3 цього Порядку, здійснюється національним органом України з акредитації відповідно до стандарту ДСТУ EN ISO/IEC 17011:2019 (EN ISO/IEC 17011:2017, IDT;

ISO/IEC 17011:2017, IDT) “Оцінка відповідності. Загальні вимоги до органів з акредитації, що акредитують органи з оцінки відповідності”.

5. Національний орган України з акредитації забезпечує, щоб атестати про акредитацію, які він видає органам з оцінки відповідності, містили таку інформацію:

1) унікальний ідентифікаційний код атестата про акредитацію;

2) дату видачі атестата про акредитацію;

3) найменування національного органу України з акредитації, який видає атестат про акредитацію;

4) найменування та код за ЄДРПОУ (код/номер з торговельного, банківського чи судового реєстру, що ведеться країною резидентства іноземної юридичної особи, код/номер з реєстраційного посвідчення місцевого органу влади іноземної держави про реєстрацію юридичної особи) акредитованого органу з оцінки відповідності;

5) сферу акредитації стосовно однієї або декількох кваліфікованих електронних довірчих послуг, визначених частиною третьою статті 16 Закону України “Про електронну ідентифікацію та електронні довірчі послуги” (далі − Закон);

6) про ідентифікацію, включаючи, за наявності, конкретну версію, схеми оцінки відповідності, щодо якої орган з оцінки відповідності був акредитований;

7) щодо зазначення використання акредитації з гнучкою сферою, за наявності;

8) ідентифікацію, за наявності, документа, що визначає процес проектування та впровадження акредитації з гнучкою сферою.

6. Національний орган України з акредитації забезпечує, щоб дата початку, а також дата завершення акредитації органу з оцінки відповідності (за наявності) для проведення оцінки відповідності кваліфікованих електронних довірчих послуг (включаючи конкретні дати для кожної окремої послуги) були частиною відомостей реєстру акредитованих органів з оцінки відповідності, який ведеться таким органом відповідно до Закону України “Про акредитацію органів з оцінки відповідності” з урахуванням вимог Закону.

7. Національний орган України з акредитації забезпечує, щоб будь-які зміни до інформації, зазначеної у пункті 5 цього Порядку, були чітко відображені в атестаті про акредитацію.

8. Атестат про акредитацію повинен чітко описувати сферу акредитації органу з оцінки відповідності відповідно до частини третьої статті 16 Закону України “Про акредитацію органів з оцінки відповідності”.

9. Власником схеми оцінки відповідності, відповідальним за її розроблення та підтримання, є Мінцифри.

Власник схеми забезпечує проведення моніторингу змін до стандартів, відповідно до яких здійснюється акредитація органів з оцінки відповідності та проведення оцінки відповідності, а також змін до схеми оцінки відповідності, на підставі якої орган з оцінки відповідності був акредитований.

10. Власник схеми повідомляє національний орган України з акредитації про зміни, виявлені за результатами проведення моніторингу, передбаченого у пункті 9 цього Порядку.

11. Органи з оцінки відповідності забезпечують публічну доступність виданих ними сертифікатів відповідності на власному офіційному вебсайті або в іншому публічному електронному реєстрі, зокрема щодо статусу, строку дії, сфери сертифікації таких сертифікатів та відповідної кваліфікованої електронної довірчої послуги.

12. У разі залучення субпідрядника до виконання окремих видів діяльності з оцінки відповідності орган з оцінки відповідності враховує характер діяльності, що передається у субпідряд, та забезпечує відповідність субпідрядника стандартам, визначеним у додатку 1 до цього Порядку, залежно від конкретного виду такої діяльності.

13. Органи з оцінки відповідності під час прийняття рішення про сертифікацію забезпечують, щоб юридична особа, фізична особа − підприємець або кваліфікований надавач електронних довірчих послуг, яких стосується таке рішення, мали можливість подати контролюючому органу звіти про оцінку відповідності, що відповідають такому рішенню.

14. Кожна схема оцінки відповідності повинна визначати власника схеми.

15. Схема оцінки відповідності повинна відповідати типу схеми 6 стандарту ДСТУ EN ISO/IEC 17067:2014 “Оцінка відповідності. Основні положення сертифікації продукції та керівні вказівки щодо схем сертифікації продукції” та вимогам, встановленим цим Порядком.

16. Власники схем повинні забезпечити, щоб їхні схеми включали щонайменше стандарти, зазначені в додатку 2 до цього Порядку, із зазначенням року та номера версії цих стандартів.

17. Власники схем повинні забезпечити, щоб у схемі була зазначена можливість застосування акредитації з гнучкою сферою, у разі застосування такої акредитації.

18. Власники схем повинні забезпечити, щоб їхні схеми включали процеси та процедури щонайменше щодо:

1) отримання та розгляд скарг, поданих власнику схеми щодо реалізації схеми оцінки відповідності;

2) повідомлення органом з оцінки відповідності контролюючому органу про видачу сертифікатів відповідності та будь-які зміни до них;

3) за потреби залучення субпідрядників до виконання органом з оцінки відповідності діяльності з оцінки відповідності;

4) проведення щорічного наглядового оцінювання відповідно до вимог пункту 7.9 стандарту ДСТУ EN ISO/IEC 17065:2019 (EN ISO/IEC 17065:2012, IDT; ISO/IEC 17065:2012, IDT) “Оцінка відповідності. Вимоги до органів з сертифікації продукції, процесів та послуг”;

5) повідомлення кваліфікованим надавачем електронних довірчих послуг органу з оцінки відповідності та контролюючому органу про будь-які зміни, що впливають на діяльність кваліфікованих надавачів електронних довірчих послуг або наданих ними кваліфікованих електронних довірчих послуг;

6) верифікації доказів, які підтверджують, що орган з оцінки відповідності:

має достатні знання та досвід щодо застосування зазначених у додатку 2 цього Порядку стандартів, пов’язаних з відповідною кваліфікованою електронною довірчою послугою;

має професійний досвід оцінки відповідності принаймні у трьох оцінках кваліфікованих надавачів електронних довірчих послуг або у трьох оцінках систем управління інформаційною безпекою;

може забезпечити наявність команди у складі не менше двох кваліфікованих осіб, що володіють необхідними знаннями для проведення такої оцінки відповідності.

19. Власники схем повинні забезпечити, щоб їхні схеми оцінки відповідності вимагали від кваліфікованих надавачів електронних довірчих послуг наявності процесів, процедур і робочих інструкцій для повідомлення органу з оцінки відповідності не пізніше ніж за один місяць до впровадження змін у наданні кваліфікованих електронних довірчих послуг, сертифікованих за такою схемою, що можуть вплинути на відповідність кваліфікованого надавача електронних довірчих послуг або відповідних послуг вимогам, відповідність яким підтверджено сертифікатом відповідності, та не пізніше ніж за три місяці до запланованої дати припинення надання таких послуг або їх частини.

20. Власники схем забезпечують, щоб схеми оцінки відповідності не дозволяли приймати позитивне рішення про сертифікацію або видавати сертифікат відповідності, якщо за результатами оцінки відповідності встановлено невідповідність юридичної особи або фізичної особи — підприємця, які мають намір надавати кваліфіковані електронні довірчі послуги, кваліфікованого надавача електронних довірчих послуг та/або відповідної кваліфікованої електронної довірчої послуги, що такою особою або надавачем надається чи має надаватися, вимогам законодавства, застосовних стандартів або відповідної схеми оцінки відповідності.

21. Власники схем забезпечують, щоб схеми оцінки відповідності встановлювали процедуру інформування про будь-яку зміну сертифіката відповідності та наслідки такої зміни для надання відповідних кваліфікованих електронних довірчих послуг.

Така процедура передбачає обов'язок кваліфікованого надавача електронних довірчих послуг негайно інформувати контролюючий орган про будь-яку зміну сертифіката відповідності, зокрема зміну його статусу, строку дії, сфери сертифікації або відповідної кваліфікованої електронної довірчої послуги.

У разі зміни сертифіката відповідності кваліфікований надавач електронних довірчих послуг зобов'язаний утримуватися від надання відповідних кваліфікованих електронних довірчих послуг та посилання на них як на кваліфіковані до підтвердження контролюючим органом їх кваліфікованого статусу.

Процедура, передбачена цим пунктом, повинна відповідати вимогам пункту 7.11 стандарту ДСТУ EN ISO/IEC 17065:2019 (EN ISO/IEC 17065:2012, IDT; ISO/IEC 17065:2012, IDT) "Оцінка відповідності. Вимоги до органів з сертифікації продукції, процесів та послуг".

22. Власники схем забезпечують, щоб їхні схеми оцінки відповідності визначали процес оцінки відповідності, який повинен проводитися протягом достатньої кількості людино-днів, та забезпечують виділення достатніх ресурсів і часу для оцінки з урахуванням обсягу та складності оцінки.

23. Власники схем повинні опублікувати стислий виклад схеми оцінки відповідності у спосіб, що забезпечує його публічну доступність для завантаження. Стислий виклад повинен містити опис набору правил і процедур, яких дотримуються для оцінки відповідності кваліфікованих надавачів електронних довірчих послуг та кваліфікованих електронних довірчих послуг, що ними надаються, вимогам законодавства у сферах електронної ідентифікації та електронних довірчих послуг, застосовних стандартів та відповідної схеми оцінки відповідності.

24. Власники схем забезпечують, щоб їхні схеми оцінки відповідності вимагали проведення принаймні одного наглядового оцінювання щороку для кожної оціненої кваліфікованої електронної довірчої послуги.

25. Будь-яка заінтересована особа має право на безоплатний доступ до актуальної та архівної інформації з реєстру акредитованих органів з оцінки відповідності щодо сфери акредитації, дати початку та, у відповідних випадках, дати завершення акредитації органу з оцінки відповідності стосовно кожного типу кваліфікованої електронної довірчої послуги, щодо якої такий орган акредитований або був акредитований для проведення оцінки відповідності. Таку інформацію надає національний орган України з акредитації.

26. Актуальна та архівна інформація, зазначена у пункті 25 цього Порядку, повинна бути доступною протягом щонайменше шести років після завершення відповідної акредитації органу з оцінки відповідності.

Додаток 1
до Порядку

Стандарти для залучення субпідрядників до діяльності з оцінки відповідності

1. ДСТУ EN ISO/IEC 17025:2019 (EN ISO/IEC 17025:2017, IDT; ISO/IEC 17025:2017, IDT) “Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій” – для діяльності з випробувань.

2. ДСТУ EN ISO/IEC 17021-1:2017 (EN ISO/IEC 17021-1:2015, IDT; ISO/IEC 17021-1:2015, IDT) “Оцінка відповідності. Вимоги до органів, які здійснюють аудит і сертифікацію систем управління. Частина 1. Вимоги” – для діяльності з аудиту систем менеджменту.

3. ДСТУ EN ISO/IEC 17020:2019 (EN ISO/IEC 17020:2012, IDT; ISO/IEC 17020:2012, IDT) “Оцінка відповідності. Вимоги до роботи різних типів органів з інспектування” – для діяльності з інспектування.

4. ДСТУ EN ISO/IEC 17065:2019 (EN ISO/IEC 17065:2012, IDT; ISO/IEC 17065:2012, IDT) “Оцінка відповідності. Вимоги до органів з сертифікації продукції, процесів та послуг” – для діяльності з оцінки відповідності.

Додаток 2
до Порядку

Стандарти для схем оцінки відповідності

Стандартами, зазначеними у пункті 16 Порядку проведення процедури акредитації органів з оцінки відповідності, які здійснюють оцінку відповідності кваліфікованих надавачів електронних довірчих послуг та кваліфікованих електронних довірчих послуг, що ними надаються, є ДСТУ ETSI TS 119 612:2026 (ETSI TS 119 612 V2.4.1 (2025-08), IDT) “Електронні підписи та інфраструктури (ESI). Довірчі списки” та такі стандарти:

Кваліфікована електронна довірча послуга	**Відповідні стандарти**
Формування кваліфікованих сертифікатів електронного підпису	ДСТУ ETSI EN 319 411-2:2026 (ETSI EN 319 411-2 V2.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2.

	Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС”; ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021–03), IDT) “Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ”; ДСТУ ETSI EN 319 412-1:2026 (ETSI EN 319 412-1 V1.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та загальні структури даних”; ДСТУ ETSI EN 319 412-2:2026 (ETSI EN 319 412-2 V2.4.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 2. Профіль сертифіката для сертифікатів, виданих фізичним особам”; ДСТУ ETSI EN 319 412-5:2026 (ETSI EN 319 412-5 V2.5.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 5. Заяви про якість”; ДСТУ ETSI TS 119 461:2026 (ETSI TS 119 461 V2.1.1 (2025-02), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для компонентів довірчих послуг, що забезпечують перевіряння особи суб'єктів довірчих послуг”; ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”
Формування кваліфікованих сертифікатів електронної печатки	ДСТУ ETSI EN 319 411-2:2026 (ETSI EN 319 411-2 V2.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС”, ДСТУ ETSI TS 119 495:2026 (ETSI TS 119 495 V1.8.1 (2026-04), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги до специфічних секторів. Профілі сертифікатів та вимоги щодо політики TSP для відкритого банкінгу”, ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021–03), IDT) “Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ”, ДСТУ

	ETSI EN 319 412-1:2026 (ETSI EN 319 412-1 V1.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та загальні структури даних”, ДСТУ ETSI EN 319 412-2:2026 (ETSI EN 319 412-2 V2.4.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 2. Профіль сертифіката для сертифікатів, виданих фізичним особам”, ДСТУ ETSI EN 319 412-3:2026 (ETSI EN 319 412-3 V1.3.1 (2023-09), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 3. Профіль сертифіката для сертифікатів, виданих юридичним особам”, ДСТУ ETSI EN 319 412-5:2026 (ETSI EN 319 412-5 V2.5.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 5. Заяви про якість”, ДСТУ ETSI TS 119 461:2026 (ETSI TS 119 461 V2.1.1 (2025-02), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для компонентів довірчих послуг, що забезпечують перевіряння особи суб'єктів довірчих послуг”, ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”
Формування кваліфікованих сертифікатів автентифікації веб-сайту	ДСТУ ETSI EN 319 411-2:2026 (ETSI EN 319 411-2 V2.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС”, ETSI TS 119 411-5, ДСТУ ETSI TS 119 495:2026 (ETSI TS 119 495 V1.8.1 (2026-04), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги до специфічних секторів. Профілі сертифікатів та вимоги щодо політики TSP для відкритого банкінгу”, ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021–03), IDT) “Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ”, ДСТУ ETSI EN 319 412-1:2026 (ETSI EN 319 412-1

	V1.6.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та загальні структури даних”, ДСТУ ETSI EN 319 412-4:2022 (ETSI EN 319 412-4 V1.2.1 (2021-11), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 4. Профіль сертифіката для сертифікатів вебсайтів”, ДСТУ ETSI EN 319 412-5:2026 (ETSI EN 319 412-5 V2.5.1 (2025-06), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 5. Заяви про якість”, ДСТУ ETSI TS 119 461:2026 (ETSI TS 119 461 V2.1.1 (2025-02), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для компонентів довірчих послуг, що забезпечують перевіряння особи суб'єктів довірчих послуг”, ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”
Перевірка кваліфікованих електронних підписів	ДСТУ ETSI TS 119 441:2026 (ETSI TS 119 441 V1.2.1 (2023-10), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики стосовно TSP, що надає послуги щодо перевіряння підписів”, ДСТУ ETSI TS 119 442:2021 (ETSI TS 119 442 V1.1.1 (2019-02), IDT) “Електронні підписи та інфраструктури (ESI). Профілі протоколів для постачальників довірчих послуг, що надають послуги перевірки цифрових підписів AdES”, ДСТУ ETSI EN 319 102-1:2026 (ETSI EN 319 102-1 V1.4.1 (2024-06), IDT) “Електронні підписи та інфраструктури (ESI). Процедури створення та перевіряння цифрових підписів AdES. Частина 1. Створення та перевіряння”, ДСТУ ETSI TS 119 102-2:2026 (ETSI TS 119 102-2 V1.4.1 (2023-06), IDT) “Електронні підписи та інфраструктури (ESI). Процедури створення та перевіряння цифрових підписів AdES. Частина 2. Звіт про перевіряння підпису”, ДСТУ ETSI TS 119 172-4:2021 (ETSI TS 119 172-4 V1.1.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Політика підписування.

	Частина 4. Правила застосування підписів (політика перевірки) для європейських кваліфікованих електронних підписів/печаток із використанням довірчих списків", ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021–03), IDT) "Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ", ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) "Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг"
Перевірка кваліфікованих електронних печаток	ДСТУ ETSI TS 119 441:2026 (ETSI TS 119 441 V1.2.1 (2023-10), IDT) "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики стосовно TSP, що надає послуги щодо перевіряння підписів", ДСТУ ETSI TS 119 442:2021 (ETSI TS 119 442 V1.1.1 (2019-02), IDT) "Електронні підписи та інфраструктури (ESI). Профілі протоколів для постачальників довірчих послуг, що надають послуги перевірки цифрових підписів AdES", ДСТУ ETSI EN 319 102-1:2026 (ETSI EN 319 102-1 V1.4.1 (2024-06), IDT) "Електронні підписи та інфраструктури (ESI). Процедури створення та перевіряння цифрових підписів AdES. Частина 1. Створення та перевіряння", ДСТУ ETSI TS 119 102-2:2026 (ETSI TS 119 102-2 V1.4.1 (2023-06), IDT) "Електронні підписи та інфраструктури (ESI). Процедури створення та перевіряння цифрових підписів AdES. Частина 2. Звіт про перевіряння підпису", ДСТУ ETSI TS 119 172-4:2021 (ETSI TS 119 172-4 V1.1.1 (2021-05), IDT) "Електронні підписи та інфраструктури (ESI). Політика підписування. Частина 4. Правила застосування підписів (політика перевірки) для європейських кваліфікованих електронних підписів/печаток із використанням довірчих списків", ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021–03), IDT) "Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ", ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) "Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг"

Зберігання кваліфікованих електронних підписів	ДСТУ ETSI TS 119 511:2019 (ETSI TS 119 511 V1.1.1 (2019-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг, що забезпечують тривале збереження цифрових підписів чи загальних даних, використовуючи методи цифрового підпису”, ДСТУ ETSI TS 119 172-4:2021 (ETSI TS 119 172-4 V1.1.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Політика підписування. Частина 4. Правила застосування підписів (політика перевірки) для європейських кваліфікованих електронних підписів/печаток із використанням довірчих списків”, ДСТУ ETSI TS 119 512:2021 (ETSI TS 119 512 V1.1.2 (2020-10), IDT) “Електронні підписи та інфраструктури (ESI). Протоколи для постачальників довірчих послуг, що надають послуги довгострокового зберігання даних”, ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021–03), IDT) “Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ”, ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”
Зберігання кваліфікованих електронних печаток	ДСТУ ETSI TS 119 511:2019 (ETSI TS 119 511 V1.1.1 (2019-06), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг, що забезпечують тривале збереження цифрових підписів чи загальних даних, використовуючи методи цифрового підпису”, ДСТУ ETSI TS 119 172-4:2021 (ETSI TS 119 172-4 V1.1.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Політика підписування. Частина 4. Правила застосування підписів (політика перевірки) для європейських кваліфікованих електронних підписів/печаток із використанням довірчих списків”, ДСТУ ETSI TS 119 512:2021 (ETSI TS 119 512 V1.1.2 (2020-10), IDT) “Електронні підписи та інфраструктури (ESI). Протоколи для постачальників довірчих послуг, що

	надають послуги довгострокового зберігання даних”, ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021–03), IDT) “Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ”, ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”
Формування кваліфікованих електронних позначок часу	ДСТУ ETSI EN 319 421:2026 (ETSI EN 319 421 V1.3.1 (2025-07), IDT) “Електронні підписи та інфраструктури (ESI). Політика та вимоги безпеки щодо надавачів довірчих послуг, які видають часові штемпелі”, ДСТУ ETSI EN 319 422:2016 (ETSI EN 319 422:2016, IDT) “Електронні підписи та інфраструктури. Протокол мітки часу та профілі токенів мітки часу”, ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021–03), IDT) “Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ”, ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”
Надання кваліфікованої електронної довірчої послуги реєстрованої електронної доставки	ДСТУ ETSI EN 319 521:2019 (ETSI EN 319 521 V1.1.1 (2019-02), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для зареєстрованих постачальників послуг електронної пошти”, ДСТУ ETSI EN 319 522-1:2018 (ETSI EN 319 522-1:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 1. Модель та архітектура”, ДСТУ ETSI EN 319 522-2:2018 (ETSI EN 319 522-2:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 2. Семантика вмісту”, ДСТУ ETSI EN 319 522-3:2018 (ETSI EN 319 522-3:2018, IDT) “Електронні підписи та інфраструктури (ESI). Служби реєстрованого електронного доставляння. Частина 3. Формати”, ДСТУ ETSI EN 319 531:2019 (ETSI EN 319 531 V1.1.1 (2019-01), IDT) “Електронні підписи та

	інфраструктури (ESI). Вимоги щодо політики та безпеки для провайдерів служби реєстрованої електронної пошти", ДСТУ ETSI EN 319 532-1:2018 (ETSI EN 319 532-1:2018, IDT) "Електронні підписи та інфраструктури (ESI). Служби реєстрованої електронної пошти (REM). Частина 1. Модель та архітектура", ДСТУ ETSI EN 319 532-2:2018 (ETSI EN 319 532-2:2018, IDT) "Електронні підписи та інфраструктури (ESI). Служби реєстрованої електронної пошти (REM). Частина 2. Семантика вмісту", ДСТУ ETSI EN 319 532-3:2022 (ETSI EN 319 532-3 V1.2.1 (2019-04), IDT) "Електронні підписи та інфраструктури (ESI). Послуги зареєстрованої електронної пошти (REM). Частина 3. Формати", ДСТУ ETSI EN 319 532-4:2022 (ETSI EN 319 532-4 V1.2.1 (2022-05), IDT) "Електронні підписи та інфраструктури (ESI). Послуги зареєстрованої електронної пошти (REM). Частина 4. Профілі сумісності", ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021–03), IDT) "Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ", ДСТУ ETSI TS 119 461:2026 (ETSI TS 119 461 V2.1.1 (2025-02), IDT) "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для компонентів довірчих послуг, що забезпечують перевіряння особи суб'єктів довірчих послуг", ДСТУ ETSI EN 319 401:2026 (ETSI EN 319 401 V3.2.1 (2026-01), IDT) "Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг"
Перевірка кваліфікованих сертифікатів автентифікації веб-сайту	Відповідно до загальних вимог перевірки та стандартів для сертифікатів автентифікації веб-сайтів (ДСТУ ETSI EN 319 411-2:2026 (ETSI EN 319 411-2 V2.6.1 (2025-06), IDT) "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС")

5. У постанові Кабінету Міністрів України від 12 грудня 2023 р. № 1298 “Про затвердження вимог до форматів удосконалених електронних підписів та печаток, які використовуються для надання електронних публічних послуг, та вимог до створення та перевірки удосконалених електронних підписів та печаток, що базуються на кваліфікованих сертифікатах відкритих ключів” (Офіційний вісник України, 2024 р., № 7, ст. 326):

1) у вимогах до форматів удосконалених електронних підписів та печаток, які використовуються для надання електронних публічних послуг, затверджених зазначеною постановою:

пункт 2 після абзацу другого доповнити новим абзацом такого змісту:

“засіб підтвердження удосконаленого електронного підпису та печатки − програмний, апаратно-програмний засіб, інформаційна або інформаційно-комунікаційна система, електронний сервіс чи їх сукупність, що забезпечує підтвердження дійсності удосконаленого електронного підпису чи печатки та надання користувачу електронних довірчих послуг результату такого підтвердження;”.

У зв’язку з цим абзаци третій − п’ятий вважати відповідно абзацами четвертим − шостим;

у пункті 3 слова та цифри “у пунктах 7-21 додатка” замінити словами та цифрами “у пунктах 7-25 додатка до цих вимог”;

пункт 5 викласти в такій редакції:

“5. Удосконалені електронні підписи та печатки, які використовуються для отримання електронних публічних послуг, створюються у форматах або за допомогою контейнера удосконалених електронних підписів та печаток, що відповідають стандартам, визначеним у додатку до цих вимог, незалежно від дати їх створення.

Удосконалені електронні підписи та печатки, створені у форматах, або за допомогою контейнерів удосконалених електронних підписів та печаток, що не відповідають стандартам, визначеним у додатку до цих вимог, можуть використовуватися для отримання електронних публічних послуг, якщо надавач електронних довірчих послуг відповідає вимогам, визначеним частиною четвертою статті 13 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”, а засоби підтвердження удосконаленого електронного підпису та печатки:

1) доступні для використання;

2) відповідають пункту 5 вимог до створення та перевірки удосконалених електронних підписів та печаток, що базуються на кваліфікованих сертифікатах відкритих ключів, затверджених постановою Кабінету Міністрів України від 12 грудня 2023 р. № 1298 “Про затвердження вимог до форматів удосконалених електронних підписів та печаток, які використовуються для надання

електронних публічних послуг, та вимог до створення та перевірки удосконалених електронних підписів та печаток, що базуються на кваліфікованих сертифікатах відкритих ключів” (Офіційний вісник України, 2024 р., № 7, ст. 326).”;

додаток до вимог викласти в такій редакції:

“Додаток
до вимог до форматів удосконалених
електронних підписів та печаток, які
використовуються для надання
електронних публічних послуг

1. ДСТУ ETSI TS 119 101:2016 (ETSI TS 119 101:2016, IDT) “Електронні підписи та інфраструктури. Вимоги та політики безпеки для додатків формування та перевірки підписів”.

2. ДСТУ ETSI EN 319 102-1:2026 (ETSI EN 319 102-1 V1.4.1 (2024-06), IDT) “Електронні підписи та інфраструктури (ESI). Процедури створення та перевіряння цифрових підписів AdES. Частина 1. Створення та перевіряння”.

3. ДСТУ ETSI TS 119 172-1:2016 (ETSI TS 119 172-1:2015, IDT) “Електронні підписи та інфраструктури (ESI). Політики підпису. Частина 1. Складники та зміст документів щодо політик підпису, придатних для читання людиною”.

4. ДСТУ ETSI TS 119 172-2:2021 (ETSI TS 119 172-2 V1.1.1 (2019-12), IDT) “Електронні підписи та інфраструктури (ESI). Політика підписування. Частина 2. Формат XML для політики підписування”.

5. ДСТУ ETSI TS 119 172-3:2021 (ETSI TS 119 172-3 V1.1.1 (2019-12), IDT) “Електронні підписи та інфраструктури (ESI). Політика підписування. Частина 3. Формат ASN.1 для політики підписування”.

6. ДСТУ ETSI TS 119 192:2022 (ETSI TS 119 192 V1.1.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Уніфікований ідентифікатор ресурсу, пов’язаний з AdES”.

7. ДСТУ ETSI EN 319 132-1:2026 (ETSI EN 319 132-1 V1.3.1 (2024-07), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Частина 1. Структурні блоки та базові підписи XAdES”.

8. ДСТУ ETSI EN 319 132-2:2021 (ETSI EN 319 132-2 V1.1.1 (2016-04), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Частина 2. Розширені підписи XAdES”.

9. ДСТУ ETSI TS 119 132-3:2022 (ETSI TS 119 132-3 V1.1.1 (2021-01), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи XAdES. Частина 3. Уведення механізмів синтаксису запису доказів (ERS) у XAdES”.

10. ДСТУ ETSI EN 319 122-1:2026 (ETSI EN 319 122-1 V1.3.1 (2023-06), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Частина 1. Структурні блоки та базові підписи CAdES”.

11. ДСТУ ETSI EN 319 122-2:2021 (ETSI EN 319 122-2 V1.1.1 (2016-04), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Частина 2. Розширені підписи CAdES”.

12. ДСТУ ETSI EN 319 142-1:2026 (ETSI EN 319 142-1 V1.2.1 (2024-01), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи PAdES. Частина 1. Структурні блоки та базові підписи PAdES”.

13. ДСТУ ETSI EN 319 142-2:2016 (ETSI EN 319 142-2:2016, IDT) “Електронні підписи та інфраструктури. Цифрові підписи PAdES. Частина 2. Додаткові профілі підписів PAdES”.

14. ДСТУ ETSI EN 319 162-1:2021 (ETSI EN 319 162-1 V1.1.1 (2016-04), IDT) “Електронні підписи та інфраструктури (ESI). Контейнери пов’язаних підписів (ASiC). Частина 1. Структурні блоки та базові контейнери ASiC”.

15. ДСТУ ETSI EN 319 162-2:2021 (ETSI EN 319 162-2 V1.1.1 (2016-04), IDT) “Електронні підписи та інфраструктури (ESI). Контейнери пов’язаних підписів (ASiC). Частина 2. Додаткові контейнери ASiC”.

16. ДСТУ ETSI TS 102 778-1:2015 (ETSI TS 102 778-1:2009, IDT) “Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 1. Огляд серії PAdES - базові принципи PAdES”.

17. ДСТУ ETSI TS 102 778-2:2015 (ETSI TS 102 778-2:2009, IDT) “Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 2. Базовий PAdES - профілі, що базуються на ISO 32000-1”.

18. ДСТУ ETSI TS 102 778-3:2015 (ETSI TS 102 778-3:2010, IDT) “Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 3. Посилений PAdES - профілі PAdES-BES і PadES-EPES”.

19. ДСТУ ETSI TS 102 778-4:2015 (ETSI TS 102 778-4:2009, IDT) “Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 4. Довгостроковий PAdES - профіль PAdES LTV”.

20. ДСТУ ETSI TS 102 778-5:2015 (ETSI TS 102 778-5:2009, IDT) “Електронні підписи та інфраструктура (ESI). Профілі розширених електронних підписів PDF. Частина 5. PAdES для XML контенту - профілі для підписів XAdES”.

21. ДСТУ ETSI TS 119 182-1:2026 (ETSI TS 119 182-1 V1.2.1 (2024-07), IDT) “Електронні підписи та інфраструктури (ESI). Цифрові підписи JAdES. Частина 1. Структурні блоки та базові підписи JAdES”.

22. ДСТУ ETSI TS 103 171:2018 (ETSI TS 103 171:2012, IDT) “Електронні підписи та інфраструктури (ESI). Базовий профіль XAdES”.

23. ДСТУ ETSI TS 103 172:2018 (ETSI TS 103 172:2013, IDT) “Електронні підписи та інфраструктури (ESI). Базовий профіль PAdES”.

24. ДСТУ ETSI TS 103 173:2018 (ETSI TS 103 173:2013, IDT) “Електронні підписи та інфраструктури (ESI). Базовий профіль CAdES”.

25. ДСТУ ETSI TS 103 174:2018 (ETSI TS 103 174:2013, IDT) “Електронні підписи та інфраструктури (ESI). Базовий профіль ASiC”.”;

2) У вимогах до створення та перевірки удосконалених електронних підписів та печаток, що базуються на кваліфікованих сертифікатах відкритих ключів, затверджених зазначеною постановою:

пункт 5 викласти в такій редакції:

“5. Засоби підтвердження удосконалених електронних підписів та печаток повинні:

1) за можливості бути придатними для автоматизованої обробки;

2) давати можливість користувачу електронних довірчих послуг підтверджувати удосконалені електронні підписи та печатки он-лайн безоплатно;

3) надавати чіткі, вичерпні, зрозумілі та легкодоступні інструкції для валідації;

4) забезпечувати зазначення інформації про них у підписаних документах та/або документах з печаткою, удосконалених електронних підписах та печатках або у контейнерах електронних документів;

5) підтверджувати дійсність удосконаленого електронного підпису та печатки за умови, що:

кваліфікований сертифікат, на якому базується удосконалений електронний підпис чи печатка, був дійсним на момент створення відповідного удосконаленого електронного підпису чи печатки;

сертифікат, на якому базується удосконалений електронний підпис чи печатка, на момент створення відповідного удосконаленого електронного підпису чи печатки був кваліфікованим сертифікатом електронного підпису чи печатки відповідно до положень Закону України “Про електронну ідентифікацію та електронні довірчі послуги” і виданий кваліфікованим надавачем електронних довірчих послуг;

значення відкритого ключа відповідає його значенню, яке міститься в кваліфікованому сертифікаті електронного підпису чи печатки;

унікальний набір даних, внесений до кваліфікованого сертифіката, на якому базується удосконалений електронний підпис чи печатка, дає змогу визначити підписувача або створювача електронної печатки;

у кваліфікованому сертифікаті електронного підпису зазначено про використання в ньому псевдоніма (у разі його використання особою на момент створення удосконаленого електронного підпису);

у випадках створення удосконаленого електронного підпису та/або печатки засобом кваліфікованого електронного підпису чи печатки про використання такого засобу повідомлено користувачу електронних довірчих послуг;

порушення цілісності електронних даних, з якими пов’язаний такий удосконалений електронний підпис чи печатка, відсутнє;

дотримано вимог, встановлених частиною першою статті 17^1 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”, на момент створення удосконаленого електронного підпису чи печатки;

інформаційна та інформаційно-комунікаційна системи, що використовуються для підтвердження удосконаленого електронного підпису та печатки, надають користувачу електронних довірчих послуг правильний результат процесу підтвердження та дають йому можливість виявляти будь-які проблеми, пов’язані з інформаційною безпекою.

Інформація, зазначена в підпункті 4 пункту 5 цих вимог, має забезпечити для довіряючих сторін легкодоступність повних специфікацій методу валідації удосконаленого електронного підпису та печатки на безоплатній основі.”;

пункт 8 викласти в такій редакції:

“8. В інформаційно-комунікаційних системах, в яких функціонує програмне забезпечення створення (валідації, додавання) підпису (SCA/SVA/SAA) або управління (DA), відповідно до вимог ДСТУ ETSI TS 119 101:2016 (ETSI TS 119 101:2016, IDT) “Електронні підписи та інфраструктури. Вимоги та політики безпеки для додатків формування та перевірки підписів” впроваджується система захисту інформації, відповідно до вимог статті 8 Закону України “Про захист інформації в інформаційно-комунікаційних системах”.

Під час впровадження системи захисту інформації відповідно до вимог статті 8 Закону України “Про захист інформації в інформаційно-комунікаційних системах” вживаються заходи, визначені пунктами 7.2 - 7.6 ДСТУ ETSI TS 119 101:2016 (ETSI TS 119 101:2016, IDT) “Електронні підписи та інфраструктури. Вимоги та політики безпеки для додатків формування та перевірки підписів”.”.

6. У вимогах до Довірчого списку, затверджених постановою Кабінету Міністрів України від 11 серпня 2023 р. № 844 (Офіційний вісник України, 2023 р., № 79, ст. 4487):

1) у пункті 2:

абзац третій викласти в такій редакції:

“електронна печатка центрального засвідчувального органу − електронна печатка, спеціально призначена для засвідчення інформації в Довірчому списку, що базується на самопідписаному сертифікаті електронної печатки центрального засвідчувального органу;”;

доповнити пункт новим абзацом такого змісту:

“файл Довірчого списку TL-UA-EC − файл Довірчого списку, до якого вносяться відомості про кваліфікованих надавачів електронних довірчих послуг та кваліфіковані електронні довірчі послуги, що ними надаються, і який призначений для забезпечення використання таких послуг в Україні та під час їх транскордонного надання між Україною та Європейським Союзом.”;

у зв’язку з цим абзац шостий вважати абзацом сьомим;

2) пункт 3 викласти в такій редакції:

“3. Держателем Довірчого списку є Мінцифри.

Довірчий список створюється та опубліковується на офіційному веб-сайті центрального засвідчувального органу у вигляді трьох файлів за таким призначенням:

файл Довірчого списку, в який вносяться відомості про кваліфікованих надавачів та їх кваліфіковані електронні довірчі послуги, надання яких передбачає використання алгоритмів електронного підпису, визначених ДСТУ ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT) “Електронні підписи та інфраструктури (ESI). Криптографічні пакети”, використовується для забезпечення визнання в Україні електронних довірчих послуг кваліфікованих надавачів;

файл Довірчого списку, в який вносяться відомості про кваліфікованих надавачів та їх кваліфіковані електронні довірчі послуги, надання яких передбачає використання алгоритмів електронного підпису, визначених ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”, використовується для забезпечення визнання в Україні електронних довірчих послуг кваліфікованих надавачів;

файл Довірчого списку TL-UA-EC.

Файл Довірчого списку TL-UA-EC містить інформацію про кваліфіковані електронні довірчі послуги, відомості про які підлягають внесенню до Довірчого

списку відповідно до законодавства, з урахуванням технічних специфікацій, затверджених Мінцифри, зокрема:

формування кваліфікованих сертифікатів електронного підпису;

формування кваліфікованих сертифікатів електронної печатки;

формування кваліфікованої електронної позначки часу.

Файл Довірчого списку TL-UA-EC містить поточну та історичну інформацію про статус кваліфікованих електронних довірчих послуг з моменту внесення відповідних відомостей до такого файлу.

Внесення відомостей про кваліфікованого надавача до файлу Довірчого списку TL-UA-EC саме по собі не підтверджує статус усіх кваліфікованих електронних довірчих послуг такого кваліфікованого надавача. Статус визначається щодо кожної кваліфікованої електронної довірчої послуги окремо відповідно до відомостей, внесених до файлу Довірчого списку TL-UA-EC.

Файл Довірчого списку TL-UA-EC та електронна печатка центрального засвідчувального органу, яка накладається на такий файл, повинні відповідати технічним специфікаціям, затвердженим Мінцифри.

Структура, зміст, порядок формування, ведення, публікації та інтерпретації файлу Довірчого списку TL-UA-EC визначаються технічними специфікаціями, затвердженими Мінцифри, з урахуванням ДСТУ ETSI TS 119 612:2026 (ETSI TS 119 612 V2.4.1 (2025-08), IDT) “Електронні підписи та інфраструктури (ESI). Довірчі списки”, ДСТУ ETSI TS 119 615:2026 (ETSI TS 119 615 V1.2.1 (2023-06), IDT) “Електронні підписи та інфраструктури (ESI). Довірчі списки. Процедури використання та тлумачення національних довірчих списків держав-членів Європейського Союзу”, інших застосовних стандартів та особливостей, визначених законодавством.

Під час надання кваліфікованих електронних довірчих послуг для перевірки статусу кваліфікованої електронної довірчої послуги, яку надає кваліфікований надавач, внесений до Довірчого списку, використовуються файли Довірчого списку відповідно до ДСТУ ETSI TS 119 612:2026 (ETSI TS 119 612 V2.4.1 (2025-08), IDT) “Електронні підписи та інфраструктури (ESI). Довірчі списки”.”;

3) доповнити вимоги після пункту 3 новими пунктами 3^1, 3^2 і 3^3 такого змісту:

“3^1. Відомості про кваліфіковані електронні довірчі послуги, для надання яких використовується один і той самий відкритий ключ кваліфікованого надавача, не можуть бути внесені до різних файлів Довірчого списку.

3^2. Для засвідчення інформації у файлі Довірчого списку TL-UA-EC використовується окрема пара ключів центрального засвідчувального органу та

відповідний самопідписаний сертифікат електронної печатки центрального засвідчувального органу.

Пара ключів та самопідписаний сертифікат електронної печатки центрального засвідчувального органу, що використовуються для засвідчення інформації у файлі Довірчого списку TL-UA-EC, не використовуються для засвідчення інформації в інших файлах Довірчого списку.

3³. Відомості про кваліфіковану електронну довірчу послугу формування кваліфікованих сертифікатів електронного підпису або електронної печатки, внесені до файлу Довірчого списку TL-UA-EC, стосуються лише кваліфікованих сертифікатів електронного підпису або електронної печатки, що містять об’єктний ідентифікатор (OID) політики сертифіката, визначений Мінцифри в межах реалізації вимог стандартів, у тому числі щодо забезпечення сумісності.”;

4) доповнити вимоги пунктами 7, 8 такого змісту:

“7. У разі публікації файлу Довірчого списку TL-UA-EC у формі, придатній для сприйняття його змісту, такий файл створюється на основі відповідного файлу Довірчого списку, придатного для автоматизованої обробки, містить ті самі дані та засвідчується електронною печаткою центрального засвідчувального органу відповідно до технічних специфікацій, затверджених Мінцифри.

8. У файлі Довірчого списку TL-UA-EC та/або інформації про файл Довірчого списку TL-UA-EC зазначається інформація про спосіб визначення, набуття, зміни, зупинення, поновлення та припинення статусу електронних довірчих послуг, а також про спосіб нагляду, оцінки відповідності або акредитації, що застосовується до кваліфікованих надавачів та кваліфікованих електронних довірчих послуг, які ними надаються, в обсязі, визначеному технічними специфікаціями, затвердженими Мінцифри.”.

_____