ЗАТВЕРДЖЕНО

постановою Кабінету Міністрів України

від ____ _____ 2024 р. № _____

ВИМОГИ
до надавачів послуг електронної ідентифікації та електронних довірчих послуг

Загальні положення

1. Ці вимоги визначають організаційно-методологічні, технічні та технологічні умови, яких повинні дотримуватися надавачі послуг електронної ідентифікації (далі – надавачі ідентифікації), а також надавачі електронних довірчих послуг (кваліфіковані та некваліфіковані) (далі – надавачі), у тому числі з безпеки та захисту інформації, та їх відокремлені пункти реєстрації під час надання послуг електронної ідентифікації та електронних довірчих послуг, а також працівники надавача.

2. Дія цих вимог не поширюється на надання послуг електронної ідентифікації та електронних довірчих послуг відповідно до положень абзацу другого частини першої статті 2 Закону України “Про електронну ідентифікацію та електронні довірчі послуги” (далі – Закон).

3. У цих вимогах терміни вживаються в такому значенні:

власник веб-сайту – користувач кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту;

геш-значення – фіксовані за обсягом електронні дані, утворені шляхом перетворення електронних даних із застосуванням криптографічного алгоритму;

заявник – фізична особа, у тому числі іноземець, фізична особа-підприємець, юридична особа та їх уповноважені представники, що звернулись до надавача ідентифікації чи надавача для отримання послуг електронної ідентифікації та електронних довірчих послуг;

інформаційно-комунікаційна система центрального засвідчувального органу – сукупність інформаційних та комунікаційних систем центрального засвідчувального органу, які у процесі обробки інформації діють як єдине ціле та об’єднують програмно-технічний комплекс, що використовується під час надання електронних довірчих послуг, інші складові системи, що використовуються для ведення Довірчого списку, постачання передачі сигналів точного часу, синхронізованого із Всесвітнім координованим часом (UTC) з

використанням національної шкали часу UTC (UA), забезпечення інтероперабельності та технологічної нейтральності технічних рішень, взаємного визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів, що використовуються під час надання юридично значущих електронних послуг, досліджень поточного стану, перспектив розвитку сфери електронних довірчих послуг та виконання інших повноважень, визначених статтями 7 та 7^1 Закону, фізичне середовище, інформацію, що обробляється в цих системах, а також найманих працівників, які безпосередньо залучені в наданні послуг або обслуговують інформаційно-комунікаційну систему;

користувач засобу електронної ідентифікації – особа, якій надавач послуг електронної ідентифікації видав засіб електронної ідентифікації згідно із схемою, внесеною до переліку схем електронної ідентифікації;

онлайн-операція – будь-яка дія, технологічна схема якої передбачає наявність безперервного комунікаційного зв’язку в режимі реального часу під час її проведення;

перевірка – виїзний захід державного нагляду (контролю) за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг, що здійснюється посадовими особами контролюючого органу відповідно до їх функціональних обов’язків за місцезнаходженням надавача, центрального засвідчувального органу або засвідчувального центру;

політика сертифіката – перелік усіх правил, що застосовуються кваліфікованим надавачем електронних довірчих послуг (далі – кваліфікований надавач) у процесі надання кваліфікованих електронних довірчих послуг з формування, перевірки та підтвердження чинності кваліфікованих сертифікатів відкритих ключів;

положення сертифікаційних практик – перелік усіх практичних дій та процедур, які застосовуються для реалізації політики сертифіката кваліфікованого надавача;

програмний інтерфейс центрального засвідчувального органу – складова інформаційно-комунікаційної системи центрального засвідчувального органу для забезпечення інтероперабельності, дослідження поточного стану, перспектив розвитку сфери електронних довірчих послуг та виконання інших повноважень, визначених статтями 7 та 7^1 Закону;

публікація кваліфікованого сертифіката відкритого ключа – надання кваліфікованого сертифіката відкритого ключа користувачеві та, у разі його згоди, – іншим особам шляхом розміщення його на веб-сайті надавача;

розповсюдження інформації про статус кваліфікованого сертифіката відкритого ключа – надання вільного доступу до інформації про статус кваліфікованого сертифіката відкритого ключа;

список відкликаних сертифікатів відкритих ключів – сформований та опублікований надавачем, центральним засвідчувальним органом/засвідчувальним центром перелік кваліфікованих сертифікатів відкритих ключів, статус яких змінено на заблокований, поновлений або скасований;

статус кваліфікованого сертифіката відкритого ключа – стан кваліфікованого сертифіката відкритого ключа (чинний, заблокований, скасований) на певний момент часу;

управління статусом сертифіката – зміна статусу кваліфікованого сертифіката відкритого ключа надавачем.

4. Інші терміни вживаються у значенні, наведеному в законах України “Про електронну ідентифікацію та електронні довірчі послуги”, “Про електронні документи та електронний документообіг”, “Про електронні комунікації”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про основні засади забезпечення кібербезпеки України”, “Про регулювання містобудівної діяльності”, постанові Кабінету Міністрів України від 11 серпня 2023 р. № 844 “Про затвердження вимог до Довірчого списку” (Офіційний вісник України 2023 р., № 79, ст. 4487) та інших нормативно-правових актах у сферах електронної ідентифікації та електронних довірчих послуг.

5. Формування сертифікатів відкритих ключів повинно здійснюватись з дотриманням таких стандартів:

ДСТУ ISO/IEC 9594-8:2021 (ISO/IEC 9594-8:2020, IDT) “Інформаційні технології. Взаємозв'язок відкритих систем. Частина 8. Каталог. Структура сертифікатів відкритих ключів та атрибутів”.

ДСТУ ETSI EN 319 412-1:2021 (ETSI EN 319 412-1 V1.4.4 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та типові структури даних”.

ДСТУ ETSI EN 319 412-2:2021 (ETSI EN 319 412-2 V2.2.1 (2020-07), IDT) “Електронні підписи та інфраструктури. (ESI). Профілі сертифікатів. Частина 2. Профілі сертифікатів, виданих фізичним особам”.

ДСТУ ETSI EN 319 412-3:2021 (ETSI EN 319 412-3 V1.2.1 (2020-07), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 3. Профілі сертифікатів, виданих юридичним особам”.

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”.

Кваліфіковані надавачі мають право самостійно обирати в рамках кожної послуги, які саме стандарти вони будуть застосовувати для надання кваліфікованих електронних довірчих послуг, з переліку стандартів, що додається (далі – Перелік).

Вимоги до надавачів ідентифікації

6. Надавач ідентифікації надає послугу електронної ідентифікації за схемою, внесеною до переліку схем електронної ідентифікації.

7. Надавачі ідентифікації під час видачі засобів електронної ідентифікації мають право здійснювати перевірку інформації, яка міститься у засобі електронної ідентифікації, який видається особі, з використанням відомостей інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ України (відомостей, що містяться в Єдиному державному демографічному реєстрі, та відомостей щодо викрадених (втрачених) документів – за зверненнями громадян), Державного реєстру фізичних осіб – платників податків, Державного реєстру актів цивільного стану громадян, Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань, а також інформації з інших публічних електронних реєстрів відповідно до Закону України "Про публічні електронні реєстри", отриманих у процесі електронної взаємодії за допомогою інтегрованої системи електронної ідентифікації відповідно до статті 11^2 Закону.

8. Надання послуг електронної ідентифікації надавачами ідентифікації має здійснюватись з дотриманням таких стандартів:

ДСТУ EN ISO/IEC 29100:2022 (EN ISO/IEC 29100:2020, IDT; ISO/IEC 29100:2011, including Amd 1:2018, IDT) "Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя";

ДСТУ ISO/IEC 29101:2018 (ISO/IEC 29101:2013, IDT) "Інформаційні технології. Методи захисту. Структура архітектури забезпечення прайвесі";

ДСТУ ISO/IEC 19989-1:2023 (ISO/IEC 19989-1:2020, IDT) "Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем. Частина 1. Структура";

ДСТУ ISO/IEC 19989-2:2023 (ISO/IEC 19989-2:2020, IDT) "Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем. Частина 2. Ефективність біометричного розпізнавання";

ДСТУ ISO/IEC 24745:2023 (ISO/IEC 24745:2022, IDT) "Інформаційні технології. Кібербезпека та захист конфіденційності. Захист біометричної інформації";

ДСТУ ISO/IEC 30107-1:2023 (ISO/IEC 30107-1:2016, IDT) "Інформаційні технології. Виявлення атак на біометричне подання. Частина 1. Структура";

ДСТУ ISO/IEC 30107-2:2023 (ISO/IEC 30107-2:2017, IDT) "Інформаційні технології. Виявлення атак на біометричне подання. Частина 2. Формати даних";

ДСТУ ISO/IEC 30107-3:2023 (ISO/IEC 30107-3:2017, IDT) "Інформаційні технології. Виявлення атак на біометричне подання. Частина 3. Тестування та звітування";

ДСТУ ISO/IEC 30107-4:2023 (ISO/IEC 30107-4:2020, IDT) “Інформаційні технології. Виявлення атак на біометричне подання. Частина 4. Профіль для тестування мобільних пристроїв”;

ДСТУ ISO/IEC 29146:2023 (ISO/IEC 29146:2016, IDT) “Інформаційні технології. Методи безпеки. Структура керування доступом”;

ДСТУ ISO/IEC 15408-1:2023 ISO/IEC 15408-1:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель”;

ДСТУ ISO/IEC 15408-2:2023 (ISO/IEC 15408-2:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки”;

ДСТУ ISO/IEC 15408-3:2023 (ISO/IEC 15408-3:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення”;

ДСТУ ISO/IEC 15408-4:2023 (ISO/IEC 15408-4:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 4. Структура для визначення методів оцінювання та діяльності”;

ДСТУ ISO/IEC 15408-5:2023 (ISO/IEC 15408-5:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки”;

ДСТУ ISO/IEC 18045:2023 (ISO/IEC 18045:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Методологія оцінювання безпеки ІТ”;

ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги”;

ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки”;

ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки”;

ДСТУ ISO/IEC 27551:2023 (ISO/IEC 27551:2021, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Вимоги до автентифікації непов’язаних об’єктів на основі атрибутів”.

9. Надавачі ідентифікації забезпечують створення та функціонування свого веб-сайту.

10. Надавачі ідентифікації забезпечують розміщення на своєму веб-сайті актуальної інформації про умови отримання послуг електронної ідентифікації, а також можуть вести реєстрацію користувачів засобів електронної ідентифікації.

11. Надавачі ідентифікації під час надання послуг електронної ідентифікації мають забезпечувати дотримання положень, визначених статтею 11^2 Закону.

12. Засоби електронної ідентифікації, що надаються надавачами ідентифікації в рамках відповідних схем електронної ідентифікації, повинні відповідати рівням довіри, визначеним статтею 15 Закону.

13. Надання засобів електронної ідентифікації надавачем ідентифікації не внесених до переліку схем електронної ідентифікації забороняється.

14. Реєстрація користувачів засобів електронної ідентифікації може здійснюватися через відокремлені пункти реєстрації, які виконують свої функції з дотриманням вимог законодавства у сферах електронної ідентифікації та захисту інформації.

Вимоги до надавачів та їх працівників

15. Вимоги до працівників надавачів їх обов'язки, а також процеси та регламентні процедури, що пов'язані з генерацією та зберіганням особистих ключів надавача, визначаються з дотриманням таких стандартів:

ДСТУ ETSI EN 319 401:2022 (ETSI EN 319 401 V2.3.1 (2021-05), IDT) "Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг";

ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021-05), 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 319 411-2:2022 (ETSI EN 319 411-2 V2.4.1 (2021-11), 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 319 421:2016 (ETSI EN 319 421:2016, IDT) "Електронні підписи й інфраструктури (ESI). Політика та вимоги безпеки щодо провайдерів трастових послуг, які видають часові штемпелі".

16. Кваліфікований надавач для надання електронних довірчих послуг призначає розпорядчим актом керівника кваліфікованого надавача, адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, адміністратора безпеки, аудитора системи (далі – працівники надавача). Кваліфікований надавач має право призначити розпорядчим актом заступника керівника кваліфікованого, який виконує функції керівника

кваліфікованого надавача у разі його відсутності або за його письмовим дорученням.

17. Працівникам надавача забороняється суміщення посадових обов'язків адміністратора безпеки з посадами адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, аудитора системи.

18. Працівники надавача, повинні мати необхідні для надання електронних довірчих послуг знання, досвід і кваліфікацію.

Адміністратором сертифікації, системним адміністратором, аудитором системи може бути особа, яка має вищу освіту за спеціальністю у сферах інформаційних технологій, захисту інформації або кібербезпеки, а також стаж роботи за фахом у зазначених сферах не менше трьох років.

Адміністратором реєстрації може бути будь-яка фізична особа, яка має навички роботи з комп'ютерною технікою.

Адміністратором безпеки може бути особа, яка має стаж роботи у сфері захисту інформації або кібербезпеки не менше трьох років та відповідає хоча б одній з умов:

1) має вищу освіту за спеціальністю у сферах кібербезпеки та захисту інформації;

2) має вищу освіту за спеціальністю у сфері інформаційних технологій та отримала сертифікат про підвищення кваліфікації у сфері кібербезпеки та захисту інформації.

19. Організаційно-правовий статус керівника і працівників надавача, їх завдання та функції, права та обов'язки, відповідальність, а також професійні знання, досвід і кваліфікація визначаються функціональними обов'язками.

Функціональні обов'язки повинні містити вимоги інформаційної безпеки.

20. Керівник і працівники надавача повинні бути ознайомлені з положеннями, якими передбачені їх функціональні обов'язки, та дотримуватись завдань та функцій, визначених такими положеннями.

21. Діяльність кваліфікованих надавачів здійснюється за умови внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів, або рахунок у Національному банку – для банків – кваліфікованих надавачів, кваліфікованого надавача, створеного Національним банком) для забезпечення відшкодування шкоди, яка може бути завдана користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання кваліфікованим надавачем своїх зобов'язань або страхування відповідальності для забезпечення відшкодування такої шкоди у розмірі, визначеному частиною п'ятою статті 16 Закону.

Кваліфіковані надавачі повинні підтримувати розмір внеску на поточному рахунку із спеціальним режимом використання або розмір страхової суми в актуальному стані та у разі зміни розміру мінімальної заробітної плати або в разі відшкодування збитків, завданих користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання своїх зобов'язань, – відновити його протягом трьох місяців з дня настання таких змін.

22. Кваліфікований надавач надає кваліфіковані електронні довірчі послуги відповідно до вимог законодавства у сфері електронних довірчих послуг, а також регламенту роботи кваліфікованого надавача (далі – Регламент).

23. Регламент розробляється та затверджується до початку роботи кваліфікованого надавача.

24. Структура регламенту, у тому числі політика сертифіката та положення сертифікаційних практик, передбачені ДСТУ ETSI EN 319 401:2022 (ETSI EN 319 401 V2.3.1 (2021-05), IDT) "Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг", ДСТУ ETSI EN 319 411-1:2022 (ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021–05), IDT "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги".

25. Регламент роботи підлягає обов'язковому погодженню з Мінцифри або із Національним банком – для кваліфікованих надавачів, зазначених в абзаці першому частини першої статті 9 Закону, (далі – орган погодження).

Регламент надсилається органу погодження в електронній формі з дотриманням вимог законодавства у сферах електронного документообігу, електронної ідентифікації та електронних довірчих послуг.

До Мінцифри Регламент може надсилатись через програмний інтерфейс інформаційно-комунікаційної системи центрального засвідчувального органу.

До Національного банку Регламент може надсилатись на електронну поштову скриньку Національного банку nbu@bank.gov.ua або через систему електронної взаємодії органів виконавчої влади або систему електронної пошти Національного банку.

Строк погодження Регламенту становить 30 календарних днів після його надходження.

Підставами для відмови у погодженні Регламенту є:

виявлення у Регламенті недостовірних відомостей, пошкоджень, які не дають змоги однозначно тлумачити зміст, виправлень або дописок;

невідповідність структури Регламенту вимогам, зазначеним у пункті 24 цих Вимог.

Процедура погодження проекту регламенту проводиться безоплатно.

Регламент після погодження органом погодження затверджується керівником кваліфікованого надавача та передається до органу погодження протягом десяти робочих днів з моменту його затвердження.

Копію затвердженого Регламенту орган погодження передає Адміністрації Держспецзв'язку протягом п'яти робочих днів з моменту його отримання.

26. Для погодження змін до Регламенту кваліфікованим надавачем надсилається до органу погодження текст відповідних змін та порівняльна таблиця у спосіб, визначений у пункті 25 цих вимог (порівняльна таблиця не надсилається у разі внесення змін до Регламенту шляхом викладення в новій редакції).

27. Кваліфікований надавач самостійно визначає обсяг положень Регламенту роботи та інших документів, що підлягають розміщенню на його веб-сайті для ознайомлення користувачів електронних довірчих послуг з інформацією про умови отримання кваліфікованих електронних довірчих послуг.

28. Заява про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку та документи, що додаються до неї, можуть бути подані представником юридичної особи або фізичною особою – підприємцем, який має намір надавати кваліфіковані електронні довірчі послуги, в електронній формі:

до Мінцифри – через програмний інтерфейс центрального засвідчувального органу;

до засвідчувального центру – на електронну поштову скриньку Національного банку nbu@bank.gov.ua або через систему електронної взаємодії органів виконавчої влади або систему електронної пошти Національного банку.

29. Після вжиття вичерпних заходів для забезпечення ідентифікації та перевірки обсягу цивільної правоздатності та дієздатності представника юридичної особи або фізичної особи – підприємця, що має намір надавати кваліфіковані електронні довірчі послуги, центральний засвідчувальний орган/засвідчувальний центр розглядає заяву про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку та документи, що до неї додаються, і за результатами їх розгляду приймає рішення в порядку та у строки, що встановлені Законом.

30. Перелік електронних довірчих послуг та кваліфікованих електронних довірчих послуг визначено частинами другою та третьою статті 16 Закону.

Кожна послуга, що входить до складу електронних довірчих послуг/кваліфікованих електронних довірчих послуг може надаватися надавачем окремо або в сукупності.

31. Електронні довірчі послуги надаються користувачам електронних довірчих послуг з дотриманням стандартів, визначених такими стандартами:

ДСТУ ETSI TR 119 400:2017 (ETSI TR 119 400:2016, IDT) “Електронні підписи та інфраструктури (ESI). Настанова з використання стандартів провайдерами довірчих послуг, які підтримують цифрові підписи та пов’язані з ними послуги”.

ДСТУ ETSI EN 319 401:2022 (ETSI EN 319 401 V2.3.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”.

ДСТУ ETSI TR 119 100:2017 (ETSI TR 119 100:2016, IDT) “Електронні підписи та інфраструктури (ESI). Настанова з використання стандартів для створення та валідації підпису”.

32. Ідентифікація заявника та перевірка обсягу його цивільної правоздатності та дієздатності здійснюється відповідно до вимог статті 22 Закону та у відповідності до ДСТУ ETSI EN 319 411-1:2022 (ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021–05), IDT Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги, а також-ДСТУ ETSI EN 319 411-2:2022 (ETSI EN 319 411-2 V2.4.1 (2021–11), 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», Порядку проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг, затвердженого цією постановою.

33. Реєстрація користувачів може здійснюватися через відокремлені пункти реєстрації з дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг, а для кваліфікованих надавачів з дотриманням вимог Регламенту.

34. Кваліфікований надавач повинен забезпечити створення можливості для ознайомлення заявників з інформацією про умови отримання кваліфікованої електронної довірчої послуги.

35. На своєму веб-сайті кваліфіковані надавачі повинні забезпечити публікацію такої інформації:

1) відомості про кваліфікованого надавача;

2) дані про внесення відомостей про кваліфікованого надавача до Довірчого списку;

3) кваліфіковані сертифікати відкритих ключів кваліфікованого надавача;

4) перелік кваліфікованих електронних довірчих послуг, які надає кваліфікований надавач;

5) дані про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг;

6) форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;

7) реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;

8) відомості про обмеження під час використання кваліфікованих сертифікатів відкритих ключів користувачами;

9) дані про порядок перевірки чинності кваліфікованого сертифіката відкритого ключа, у тому числі умови перевірки статусу кваліфікованого сертифіката відкритого ключа;

10) перелік актів законодавства у сфері електронних довірчих послуг.

Кваліфікований надавач забезпечує інформування користувачів про умови отримання кваліфікованих електронних довірчих послуг, зокрема шляхом розміщення відповідної інформації на веб-сайті кваліфікованого надавача.

Інформація на веб-сайті кваліфікованого надавача повинна бути доступною для осіб з інвалідністю.

36. Кваліфікований надавач забезпечує вільний доступ до своїх приміщень, в яких здійснюється обслуговування користувачів, у тому числі створення належних умов для доступу до приміщень маломобільних груп населення.

Інформація про умови доступності таких приміщень для осіб з інвалідністю розміщується у місці, доступному для сприйняття користувачів.

37. Кваліфікований надавач зобов’язаний щороку до 15 січня подавати до Адміністрації Держспецзв’язку звіт про діяльність за попередній рік, що містить відомості про:

1) кількість укладених договорів про надання електронних довірчих послуг (окремо з фізичними та юридичними особами);

2) кількість сформованих та скасованих кваліфікованих сертифікатів відкритих ключів за звітний період із зазначенням причин скасування (у разі коли кваліфікований надавач забезпечує надання кваліфікованих електронних довірчих послуг, які передбачають обслуговування кваліфікованих сертифікатів відкритих ключів);

3) факти відшкодування шкоди користувачам електронних довірчих послуг та/або третім особам внаслідок неналежного виконання надавачем своїх зобов’язань (у разі наявності);

4) факти участі кваліфікованого надавача як позивача, відповідача або третьої сторони у судових справах з питань надання електронних довірчих послуг, предмет розгляду та прийняте рішення (у разі наявності);

5) факти порушення кваліфікованим надавачем вимог законодавства у сфері захисту інформації під час надання електронних довірчих послуг, їх причини та заходи, вжиті для усунення таких порушень.

38. Центральний засвідчувальний орган/засвідчувальний центр надає кваліфіковані електронні довірчі послуги кваліфікованим надавачам відповідно до регламенту роботи центрального засвідчувального органу/Регламенту роботи засвідчувального центру, цих вимог та з урахуванням положень, передбачених Законом.

39. Центральний засвідчувальний орган оприлюднює рішення про внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку на своєму офіційному веб-сайті, а також повідомляє про його прийняття представникові юридичної особи або фізичній особі – підприємцю, що має намір надавати кваліфіковані електронні довірчі послуги, з використанням засобів поштового зв'язку або в електронній формі через програмний інтерфейс центрального засвідчувального органу протягом трьох робочих днів з дня його прийняття.

Засвідчувальний центр оприлюднює інформацію про прийняте рішення щодо внесення відомостей про юридичну особу або фізичну особу – підприємця до Довірчого списку на своєму офіційному веб-сайті, а також повідомляє про прийняте рішення юридичну особу або фізичну особу – підприємця шляхом надсилання листа на електронну поштову скриньку, вказану у Заяві про внесення до Довірчого списку, або через систему електронної взаємодії органів виконавчої влади або систему електронної пошти Національного банку протягом трьох робочих днів з дня його прийняття.

40. Кваліфікований надавач у разі виникнення підстав, передбачених Законом для внесення змін відомостей про нього до Довірчого списку, зобов'язаний протягом п'яти робочих днів із дня настання таких підстав подати до органу, який приймав рішення про внесення відомостей про нього до Довірчого списку:

1) заяву про внесення змін до Довірчого списку разом з документами, що підтверджують відповідні зміни;

2) документи для формування кваліфікованих сертифікатів ключів кваліфікованого надавача (окремо для кожної кваліфікованої електронної довірчої послуги) відповідно до вимог Регламенту органу, який приймав рішення про внесення відомостей про нього до Довірчого списку, якщо зміни відомостей, що містяться в Довірчому списку про цього кваліфікованого надавача, пов'язані з формуванням нових сертифікатів ключів кваліфікованого надавача.

41. Кваліфікований надавач припиняє діяльність з надання кваліфікованих електронних довірчих послуг з підстав та в порядку, що визначені статтею 31 Закону.

42. Кваліфікований надавач, що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, передає обслуговування користувачів електронних довірчих послуг з якими він уклав договори про надання кваліфікованих електронних довірчих послуг, а також документовану

інформацію про цих користувачів до іншого кваліфікованого надавача у порядку відповідно до частини шостої статті 31 Закону.

43. Кваліфіковані сертифікати відкритих ключів, що формуються кваліфікованими надавачами, 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 здійснюватися з дотриманням стандартів визначених пунктом 5 цих вимог та ДСТУ ETSI EN 319 412-5:2022 (ETSI EN 319 412-5 V2.3.1 (2020-04), IDT) “Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 5. Розширення сертифікатів QCStatements”.

44. Кваліфікований надавач, центральний засвідчувальний орган, засвідчувальний центр який видав кваліфікований сертифікат відкритого ключа, забезпечує доступ до інформації про дату та час зміни статусу кваліфікованого сертифіката відкритого ключа через комунікаційні мережі загального користування.

45. Час, що використовується надавачем в інформаційно-комунікаційній системі надавача в процесі надання електронних довірчих послуг та в журналах аудиту подій в електронній формі повинен бути синхронізований із Всесвітнім координованим часом (UTC) з використанням національної шкали часу UTC (UA) з точністю до секунди.

Для кваліфікованих надавачів, відомості про яких вносяться до Довірчого списку за рішенням центрального засвідчувального органу, послуги з постачання передачі сигналів точного часу, синхронізованого із Всесвітнім координованим часом (UTC) з використанням національної шкали часу UTC (UA) надаються центральним засвідчувальним органом.

Вимоги до синхронізації часу у програмно-технічних комплексах кваліфікованих надавачів, зазначених в абзаці першому частини першої статті 9 Закону, встановлюються Національним банком.

46. Механізм синхронізації часу із Всесвітнім координованим часом (UTC) в програмно-технічному комплексі надавача та склад технічного обладнання, що застосовується у процесі синхронізації часу (його загальний опис) встановлюється Порядком синхронізації часу із Всесвітнім координованим часом (UTC) з використанням національної шкали часу UTC (UA), що розробляється надавачем.

Порядок синхронізації часу із Всесвітнім координованим часом (UTC) з використанням національної шкали часу UTC (UA) кваліфікованого надавача, відомості про якого вносяться до Довірчого списку за рішенням центрального засвідчувального органу погоджується з Мінцифри.

Вимоги до надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток, а також порядок перевірки їх дотримання

47. Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печаток включає вчинення дій, передбачених частиною першою статті 18 Закону, а також здійснюється з дотриманням таких стандартів:

ДСТУ ETSI TR 119 000:2017 (ETSI TR 119 000:2016, IDT) “Електронні підписи та інфраструктури (ESI). Модель стандартизації підписів. Огляд”.

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”.

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”.

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 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT) “Електронні підписи та інфраструктури (ESI). Криптографічні пакети”.

48. Під час надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих електронних підписів чи печаток кваліфікованим надавачем забезпечується:

1) використання підписувачем або створювачем електронної печатки виключно засобу кваліфікованого електронного підпису чи печатки та кваліфікованого сертифіката електронного підпису чи печатки;

2) захист обміну інформацією між підписувачем або створювачем електронної печатки та кваліфікованим надавачем засобами електронних комунікаційних мереж загального користування;

3) створення умов для генерації пари ключів підписувача або створювача електронної печатки;

4) допомога під час генерації пари ключів підписувача або створювача електронної печатки у спосіб, що не допускає порушення конфіденційності та цілісності особистого ключа, а також ознайомлення із значенням параметрів особистого ключа та їх копіювання;

5) унікальність пари ключів підписувача або створювача електронної печатки;

6) зберігання особистого ключа підписувача або створювача електронної печатки у засобі кваліфікованого електронного підпису чи печатки;

7) захист від доступу сторонніх осіб до параметрів особистого ключа підписувача або створювача електронної печатки під час використання засобу кваліфікованого електронного підпису чи печатки.

49. У разі коли пара ключів була згенерована заявником поза приміщенням надавача та/або за відсутності відповідного персоналу, ідентифікація такого заявника, перевірка обсягу його цивільної правоздатності і дієздатності, формування та видача йому кваліфікованого сертифіката відкритого ключа здійснюється кваліфікованим надавачем після перевірки факту володіння заявником особистим ключем, який відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката відкритого ключа.

Перевірка факту володіння заявником особистим ключем здійснюється без розкриття його особистого ключа.

50. Генерацію та/або управління парою ключів від імені підписувача або створювача електронної печатки може здійснювати виключно кваліфікований надавач.

51. Кваліфікований надавач, який здійснює управління парою ключів підписувача або створювача електронної печатки, може здійснювати резервне копіювання особистого ключа підписувача або створювача електронної печатки з метою його зберігання за умови дотримання таких вимог:

1) рівень безпеки резервної копії особистого ключа повинен відповідати рівню безпеки оригінального особистого ключа;

2) кількість резервних копій не повинна перевищувати мінімального значення, необхідного для забезпечення безперервності послуги.

52. Кваліфікований електронний підпис чи печатка повинні відповідати таким вимогам:

1) бути однозначно пов’язаним (пов’язаною) з підписувачем або створювачем електронної печатки;

2) надавати можливість здійснити електронну ідентифікацію підписувача або створювача електронної печатки;

3) створюватися з використанням засобу кваліфікованого електронного підпису чи печатки,

4) базуватися на кваліфікованому сертифікаті відкритого ключа;

5) бути пов’язаним (пов’язаною) з електронними даними, на які накладено кваліфікований електронний підпис чи печатку, таким чином, щоб будь-яка наступна зміна таких даних могла бути виявлена.

53. Перевірка кваліфікованого електронного підпису чи печатки проводиться будь-якою особою з метою отримання інформації про дійсність чи недійсність кваліфікованого електронного підпису чи печатки.

54. У процесі перевірки кваліфікованого електронного підпису чи печатки підтвердження таких підпису чи печатки здійснюється за умови дотримання вимог, визначених у частині другій статті 18 Закону та у пункті 52 цих вимог, на момент накладення підпису чи печатки на пов’язані електронні дані;

55. Надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток передбачає, що така послуга:

1) надається виключно кваліфікованим надавачем;

2) відповідає всім вимогам до перевірки кваліфікованих електронних підписів чи печаток, визначеним у пункті 54 цих вимог;

3) дає змогу отримувати результати перевірки із застосуванням щонайменше удосконаленого електронного підпису чи печатки надавача автоматизованим способом, який є надійним, ефективним та захищеним.

56. Державний нагляд (контроль) за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг здійснює контролюючий орган.

Функції контролюючого органу виконує Державна служба спеціального зв’язку та захисту інформації України.

Контролюючий орган здійснює виїзні та невиїзні заходи державного нагляду (контролю).

Контролюючий орган може подати запит до органу з оцінки відповідності про надання аудиторського звіту щодо проведення процедури оцінки відповідності відповідно до вимог статті 32 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

57. Контролюючий орган здійснює позапланові заходи державного нагляду (контролю) за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг у випадках, визначених частиною третьою статті 33^1 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

У разі негативних результатів оцінки відповідності та/або наданих органом з оцінки відповідності рекомендацій контролюючий орган вживає заходи, передбачені частиною першою статті 33^1 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

58. Невиїзні заходи державного нагляду (контролю) за дотриманням вимог законодавства у сферах електронної ідентифікації та/або електронних довірчих послуг контролюючий орган здійснює відповідно до статті 34^1 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

59. Предметом перевірки надавача, центрального засвідчувального органу або засвідчувального центру є стан дотримання ними вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг.

Організація проведення перевірки контролюючим органом та оформлення її результатів здійснюються відповідно до статей 34^2 -34^7 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

60. Контролюючий орган за результатами проведення перевірок надавачів, засвідчувального центру, центрального засвідчувального органу вживає заходів реагування, передбачених статтями 33^2, 34^8-34^{10} Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

61. Контролюючий орган на підставах і в порядку, встановлених законами та міжнародними договорами України, у межах своїх повноважень співпрацює з уповноваженими органами іноземних держав, надає їм допомогу та звертається до них за отриманням допомоги з питань нагляду і контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг.

Вимоги до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, а також порядок перевірки їх дотримання

62. Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки включає вчинення дій, передбачених частиною першою статті 20 Закону, а також здійснюється з дотриманням таких стандартів:

ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021-05), 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 319 411-2:2022 (ETSI EN 319 411-2 V2.4.1 (2021-11), 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”.

63. Формування кваліфікованого сертифіката електронного підпису чи печатки заявника може здійснюватися кваліфікованим надавачем на основі ідентифікаційних даних особи отриманих з використанням відомостей інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ України (відомостей, що містяться в Єдиному державному демографічному реєстрі, та відомостей щодо викрадених (втрачених) документів за зверненнями громадян), Державного реєстру фізичних осіб – платників податків, Державного реєстру актів цивільного стану громадян, Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань, а також інформації з інших публічних електронних реєстрів відповідно до Закону України “Про публічні електронні реєстри”, отриманих у процесі електронної взаємодії за допомогою інтегрованої системи електронної ідентифікації відповідно до частини першої статті 13 Закону.

64. У разі зміни відомостей, що містяться у кваліфікованому сертифікаті електронного підпису чи печатки, користувач електронних довірчих послуг протягом трьох робочих днів з дня настання таких змін повідомляє про це кваліфікованого надавача.

На підставі наданих користувачем електронних довірчих послуг документів, що підтверджують зміни відомостей, які містяться у кваліфікованому сертифікаті електронного підпису чи печатки, кваліфікований надавач здійснює повторне формування такого сертифіката та його публікацію у разі згоди користувача електронних довірчих послуг.

Повторне формування кваліфікованого сертифіката електронного підпису чи печатки користувача електронних довірчих послуг не продовжує строку його дії.

65. Сформований кваліфікований сертифікат електронного підпису чи печатки користувача електронних довірчих послуг скасовується або блокується кваліфікованим надавачем у разі наявності підстав, передбачених статтею 25 Закону.

Під час опрацювання заяви про скасування або блокування кваліфікованого сертифіката електронного підпису чи печатки кваліфікованим надавачем здійснюється ідентифікація та перевірка обсягу цивільної правоздатності і дієздатності користувача електронних довірчих послуг з дотриманням вимог щодо підтвердження особи, встановлених у Регламенті.

66. Кваліфікований сертифікат електронного підпису чи печатки користувача електронних довірчих послуг вважається скасованим або заблокованим з моменту зміни надавачем статусу кваліфікованого сертифіката електронного підпису чи печатки користувача електронних довірчих послуг на скасований або заблокований.

67. Користувач електронних довірчих послуг, статус кваліфікованого сертифіката електронного підпису чи печатки якого було змінено на скасований чи заблокований, повинен невідкладно бути поінформований про відповідну зміну статусу.

68. Скасований кваліфікований сертифікат електронного підпису чи печатки поновленню не підлягає.

69. Відомості про кваліфіковані сертифікати електронного підпису чи печатки, сформовані кваліфікованим надавачем, їх статус та списки відкликаних сертифікатів відкритих ключів містяться у реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів.

70. Розповсюдження інформації про статус кваліфікованих сертифікатів електронного підпису чи печатки користувачів електронних довірчих послуг здійснюється шляхом публікації повного та часткового списків відкликаних сертифікатів відкритих ключів на веб-сайті кваліфікованого надавача та забезпечення створення можливості перевірки статусу кваліфікованого

сертифіката електронного підпису чи печатки користувача електронних довірчих послуг в режимі реального часу через електронні комунікаційні мережі загального користування.

Список відкликаних сертифікатів відкритих ключів надавача повинен відповідати таким вимогам:

у кожному списку відкликаних сертифікатів відкритих ключів зазначається строк його дії до видання нового списку, якщо інше не передбачено Регламентом;

новий список відкликаних сертифікатів відкритих ключів може бути опубліковано до закінчення строку його дії та видання наступного списку;

на список відкликаних сертифікатів відкритих ключів повинен бути накладений кваліфікований електронний підпис чи печатка кваліфікованого надавача.

71. Управління статусом кваліфікованого сертифіката електронного підпису чи печатки та поширення відповідної інформації повинні бути доступні для користувача електронних довірчих послуг цілодобово.

72. Заява про скасування або блокування кваліфікованого сертифіката електронного підпису чи печатки фіксується та зберігається кваліфікованим надавачем протягом строку, визначеного законодавством у сфері архівної справи для зберігання документованої інформації.

73. Кваліфікований надавач повинен забезпечити цілісність та походження інформації про статус кваліфікованих сертифікатів електронного підпису чи печатки.

74. Формування кваліфікованого сертифіката електронного підпису чи печатки здійснюється кваліфікованим надавачем за запитом користувача електронних довірчих послуг.

75. Кваліфіковані надавачі отримують кваліфіковану електронну довірчу послугу з формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки від центрального засвідчувального органу.

Кваліфіковані надавачі, що вносяться до Довірчого списку за поданням засвідчувального центру, отримують кваліфіковану електронну довірчу послугу з формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки від засвідчувального центру.

76. Перевірка дотримання вимог до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки здійснюється у порядку, визначеному пунктами 56-61 цих Вимог.

Вимоги до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту, а також порядок перевірки їх дотримання

77. Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту включає вчинення дій, передбачених частиною першою статті 21 Закону, та з дотриманням стандартів, визначених такими стандартами:

ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021-05), 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 319 411-2:2022 (ETSI EN 319 411-2 V2.4.1 (2021-11), 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 319 412-4:2022 (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”.

78. Формування кваліфікованого сертифіката автентифікації веб-сайту здійснюється кваліфікованим надавачем за запитом користувача електронних довірчих послуг.

79. Кваліфікований сертифікат автентифікації веб-сайту забезпечує:

1) автентифікацію власника веб-сайту;

2) гарантування:

шифрування інформації, обмін якою здійснюється через мережу Інтернет учасником онлайн-операції та веб-сайтом;

належного рівня довіри до власника веб-сайту щодо захисту від шахрайства в мережі Інтернеті;

захисту особистої інформації та персональних даних учасника онлайн-операції під час проведення такої операції.

80. Перевірка кваліфікованого сертифіката автентифікації веб-сайту може проводитися будь-якою особою з метою отримання інформації про власника веб-сайту та чинності кваліфікованого сертифіката автентифікації веб-сайту.

81. Під час перевірки кваліфікованого сертифіката автентифікації веб-сайту особа, що проводить перевірку, вчиняє такі дії:

1) отримує з кваліфікованого сертифіката автентифікації веб-сайту інформацію, що містить ідентифікаційні дані особи, які дають змогу однозначно встановити власника веб-сайту та кваліфікованого надавача;

2) перевіряє кваліфікований електронний підпис чи печатку, накладений на кваліфікований сертифікат автентифікації веб-сайту, за допомогою чинного (на момент формування кваліфікованого сертифіката автентифікації веб-сайту) кваліфікованого сертифіката відкритого ключа надавача.

82. Кваліфікований сертифікат автентифікації веб-сайту вважається чинним у разі відповідності вимогам, установленим частиною першою статті 24 Закону.

83. Кваліфіковані надавачі отримують кваліфіковану електронну довірчу послугу з формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту від центрального засвідчувального органу.

84. Перевірка дотримання вимог до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту здійснюється у порядку, визначеному пунктами 56-61 цих Вимог.

Особливості створення електронного підпису та електронної печатки іншого призначення

85. Кваліфіковані надавачі можуть формувати та видавати кваліфіковані сертифікати відкритого ключа іншого призначення, ніж для автентифікації веб-сайту, створення електронного підпису та електронної печатки.

86. У запиті на формування кваліфікованих сертифікатів відкритого ключа іншого призначення користувач електронних довірчих послуг вказує призначення такого ключа.

87. Процедура формування, блокування та скасування кваліфікованих сертифікатів відкритого ключа іншого призначення така ж як і для сертифікатів електронного підпису та електронної печатки.

Вимоги до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження кваліфікованої електронної позначки часу, а також порядок перевірки їх дотримання

88. Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження кваліфікованої електронної позначки часу включає вчинення дій, передбачених частиною першою статті 26 Закону, та з дотриманням стандартів, визначених такими стандартами:

ДСТУ ETSI EN 319 401:2022 (ETSI EN 319 401 V2.3.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг”.

ДСТУ ETSI EN 319 421:2016 (ETSI EN 319 421:2016, IDT) “Електронні підписи й інфраструктури (ESI). Політика та вимоги безпеки щодо провайдерів трастових 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”.

89. Перевірка кваліфікованої електронної позначки часу може проводитися будь-якою особою з метою отримання інформації про чинність кваліфікованої електронної позначки часу.

90. Перевірка дотримання вимог до надання кваліфікованої електронної довірчої послуги з формування, перевірки та підтвердження кваліфікованої електронної позначки часу здійснюється у порядку, визначеному пунктами 56-61 цих Вимог.

Вимоги до надання кваліфікованої електронної довірчої послуги реєстрованої електронної доставки, а також порядок перевірки їх дотримання

91. Кваліфікована електронна довірча послуга реєстрованої електронної доставки повинна відповідати вимогам, передбаченим частиною першою статті 27 Закону, та з дотриманням стандартів, визначених такими стандартами:

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”.

92. Кваліфікована електронна довірча послуга реєстрованої електронної доставки повинна та включати такі дії:

1) відправку електронних даних із забезпеченням доказів відправки;

2) отримання електронних даних із забезпеченням доказів отримання.

93. Реєстрована електронна доставка здійснюється кваліфікованим надавачем за запитом користувача електронних довірчих послуг (відправника та/або отримувача електронних даних).

94. Перевірка електронних даних, що передаються в процесі реєстрованої електронної доставки, проводиться отримувачем електронних даних.

95. Перевірка дотримання вимог до надання кваліфікованої електронної довірчої послуги реєстрованої електронної доставки здійснюється у порядку, визначеному пунктами 56-61 цих Вимог.

Вимоги до надання кваліфікованої електронної довірчої послуги із зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, а також порядок перевірки їх дотримання

96. Кваліфікована електронна довірча послуга із зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами, повинна надаватись з дотриманням положень статті 28 Закону та стандартів 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" та 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".

97. Зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів здійснюється кваліфікованим надавачем за запитом користувача електронних довірчих послуг.

98. Під час надання кваліфікованої електронної довірчої послуги із зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів забезпечується:

1) цілісність всіх збережених об'єктів даних;

2) протоколювання подій на предмет зміни, видалення або додавання об'єктів даних;

3) покладення відповідальності за їх зберігання на одну чи декілька посадових осіб;

4) проведення перевірок дотримання зазначених вимог.

99. Перевірка дотримання вимог до надання кваліфікованої електронної довірчої послуги із зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами здійснюється у порядку, визначеному пунктами 56-61 цих Вимог.

Перелік змін у наданні кваліфікованих електронних довірчих послуг, про які кваліфіковані надавачі зобов'язані поінформувати контролюючий орган та центральний засвідчувальний орган або засвідчувальний центр

100. Кваліфіковані надавачі зобов'язані поінформувати контролюючий орган та центральний засвідчувальний орган або засвідчувальний центр, в тому числі, але не виключно у зв'язку із введенням надзвичайного стану, воєнного стану чи виникненням іншої надзвичайної ситуації, протягом 48 годин з моменту настання таких обставин в своїй діяльності:

1) припинення надання однієї чи декількох кваліфікованих електронних довірчих послуг, відомості про які внесені до Довірчого списку;

2) змін в складі інформаційно-комунікаційної системи кваліфікованого надавача, які відбулися з порушенням вимог документа про відповідність Надавача, отриманого за результатами проходження процедури оцінки відповідності у сфері електронних довірчих послуг;

3) отримання атестату відповідності комплексної системи захисту інформації інформаційно-комунікаційної системи, що діє протягом визначеного в ньому строку дії, але не більше п'яти років з дня набрання чинності Законом;

4) проходження додаткової державної експертизи комплексної системи захисту інформації, що діє протягом визначеного в ньому строку дії, але не більше п'яти років з дня набрання чинності Законом або процедури оцінки відповідності інформаційно-комунікаційної системи кваліфікованого надавача у разі модернізації апаратного, апаратно-програмного пристрою чи програмного забезпечення, що входять до складу програмно-технічного комплексу, яка не передбачена проектною чи експлуатаційною документацією до комплексної системи захисту інформації інформаційно-комунікаційної системи кваліфікованого надавача;

5) змін щодо способів ідентифікації особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа;

6) змін щодо процедури формування, блокування, скасування, поновлення кваліфікованих сертифікатів відкритих ключів користувачів електронних довірчих послуг;

7) змін щодо процедури надання інформації про статус кваліфікованих сертифікатів відкритих ключів користувачів електронних довірчих послуг;

8) змін щодо умови використання засобів кваліфікованого електронного підпису чи печатки;

9) укладення договору страхування відповідальності або поповнення/списання коштів на поточному рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів, або рахунку у Національному банку – для банків – кваліфікованих надавачів, кваліфікованого надавача, створеного Національним банком) для забезпечення відшкодування збитків, які

можуть бути заподіяні кваліфікованим надавачем користувачам електронних довірчих послуг внаслідок неналежного виконання своїх обов’язків.

101. Інформування контролюючого органу та центрального засвідчувального органу або засвідчувального центру про настання змін в діяльності кваліфікованого надавача здійснюється в паперовій або в електронній формі.

Вимоги з безпеки та захисту інформації надавачів та надавачів ідентифікації

102. Діяльність з безпеки та захисту інформації надавачів та надавачів ідентифікації (відокремлених пунктів реєстрації) організовується, постійно підтримується та координується службою захисту інформації з дотриманням вимог законодавства у сфері захисту інформації, електронної ідентифікації та електронних довірчих послуг, Регламенту, а також з дотриманням вимог таких стандартів:

ДСТУ EN 419211-1:2016 (EN 419211-1:2014, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 1. Огляд”.

ДСТУ EN 419211-2:2016 (EN 419211-2:2013, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 2. Пристрій з генерацією ключів”.

ДСТУ EN 419211-3:2016 (EN 419211-3:2013, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 3. Пристрій з імпортом ключів”.

ДСТУ EN 419211-4:2016 (EN 419211-4:2013, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 4. Розширення для пристроїв з генерацією ключів та довіреним каналом для застосування генерації сертифікатів”.

ДСТУ EN 419211-5:2016 (EN 419211-5:2013, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 5. Розширення для пристроїв з генерацією ключів та довіреним каналом для застосування створення підпису”.

ДСТУ EN 419211-6:2016 (EN 419211-6:2014, IDT) “Профілі захисту для пристроїв створення безпечного підпису. Частина 6. Розширення для пристроїв з імпортом ключів та довіреним каналом для застосування створення підпису”.

ДСТУ ISO/IEC 19790:2015 (ISO/IEC 19790:2012, IDT) “Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів”.

ДСТУ EN 419221-5:2018 (EN 419221-5:2018, IDT) “Профілі захисту для криптографічних модулів TSP. Частина 5. Криптографічний модуль для довірчих послуг”.

ДСТУ CEN/TS 419221-6:2021 (CEN/TS 419221-6:2019, IDT) “Умови застосування EN 419221-5 як кваліфікованого пристрою для створення електронного підпису або печатки”.

ДСТУ EN 419231:2021 (EN 419231:2019, IDT) “Профіль захисту для надійних систем, що підтримують відмітку часу”.

ДСТУ EN 419241-1:2021 (EN 419241-1:2018, IDT) “Надійні системи, що підтримують підписи серверів. Частина 1. Загальні вимоги щодо безпеки системи”.

ДСТУ EN 419241-2:2021 (EN 419241-2:2019, IDT) “Надійні системи, що підтримують підписи серверів. Частина 2. Профіль захисту для QSCD для підписів серверів”.

ДСТУ ETSI TS 119 431-1:2022 (ETSI TS 119 431-1 V1.2.1 (2021-05), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг. Частина 1. Компоненти сервісу TSP, що працюють віддаленим QSCD/SCDev”.

ДСТУ ETSI TS 119 431-2:2019 (ETSI TS 119 431-2 V1.1.1 (2018-12), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для постачальників довірчих послуг. Частина 2. Компоненти сервісу TSP, що підтримують створення цифрового підпису AdES”.

ДСТУ ETSI TS 119 432-2:2022 (ETSI TS 119 432 V1.2.1 (2020-10), IDT) “Електронні підписи та інфраструктури (ESI). Протоколи віддаленого створення цифрового підпису”.

ДСТУ ETSI TS 119 495:2022 (ETSI TS 119 495 V1.5.1 (2021-04), IDT) “Електронні підписи та інфраструктури (ESI). Секторальні специфічні вимоги. Профілі сертифікатів і вимоги політики TSP для відкритого банківського обслуговування”.

ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”.

ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хэширования”.

ДСТУ 7564:2014 “Інформаційні технології. Криптографічний захист інформації. Функція ґешування”.

ДСТУ 7624:2014 “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення”.

ДСТУ ETSI TR 103 570:2022 (ETSI TR 103 570 V1.1.1 (2017-10), IDT) “Кібербезпека. Квантово-безпечний обмін ключами”.

ДСТУ ETSI TR 103 616:2022 (ETSI TR 103 616 V1.1.1 (2021-09), IDT) “Кібербезпека. Квантово-безпечні підписи”.

ДСТУ ETSI TR 103 823:2022 (ETSI TR 103 823 V1.1.2 (2021-10), IDT) “Кібербезпека. Квантово-безпечне шифрування з відкритим ключем та інкапсуляція ключів”.

ДСТУ ETSI TR 119 300:2016 (ETSI TR 119 300:2016, IDT) “Електронні підписи та інфраструктури (ESI). Настанова щодо застосування стандартів для криптографічних комплектів”.

ДСТУ ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT) “Електронні підписи та інфраструктури (ESI). Криптографічні пакети”.

ДСТУ ISO/IEC 14888-1:2015 (ISO/IEC 14888-1:2008, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення”.

ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел”.

ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT) “Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі дискретного логарифмування”.

ДСТУ ISO/IEC 18032:2022 (ISO/IEC 18032:2020, IDT) “Інформаційні технології. Методи захисту. Генерування простого числа”.

ДСТУ ISO/IEC 18033-6:2022 (ISO/IEC 18033-6:2019, IDT) “Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 6. Гомоморфне шифрування”.

ДСТУ ISO/IEC 19772:2022 (ISO/IEC 19772:2020, IDT) “Інформаційна безпека. Автентифіковане шифрування”.

ДСТУ ISO/IEC 18045:2015 (ISO/IEC 18045:2008, IDT) “Інформаційні технології. Методи захисту. Методологія оцінювання безпеки ІТ”.

ДСТУ ISO/IEC 15408-1:2023 ISO/IEC 15408-1:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель”.

ДСТУ ISO/IEC 15408-2:2023 (ISO/IEC 15408-2:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки”.

ДСТУ ISO/IEC 15408-3:2023 (ISO/IEC 15408-3:2022, IDT) “Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення”.

ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги”.

ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки”.

ДСТУ ISO/IEC 27701:2022 (ISO/IEC 27701:2019, IDT) “Методи безпеки. Розширення до ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови”.

ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки”.

103. Інформаційно-комунікаційні системи кваліфікованих надавачів та надавачів ідентифікації, що використовуються ними під час надання послуг електронної ідентифікації та електронних довірчих послуг повинні відповідати вимогам із захисту інформації шляхом впровадження комплексної системи захисту інформації або системи управління інформаційною безпекою з підтвердженою відповідністю з дотриманням вимог законодавства у сфері захисту інформації та цього розділу.

104. Надання кваліфікованих електронних довірчих послуг та здійснення реєстрації користувачів без чинних документів, що підтверджують відповідність комплексної системи захисту інформації або системи управління інформаційною безпекою з підтвердженою відповідністю, вимогам законодавства у сфері захисту інформації, забороняється.

105. Використання у засобах кваліфікованого електронного підпису криптографічних алгоритмів, визначених стандартами ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”; ГОСТ 34.311-95 “Информационная технология. Криптографическая защита информации. Функция хэширования”; ДСТУ 7564:2014 “Інформаційні технології. Криптографічний захист інформації. Функція ґешування”; ДСТУ 7624:2014 “Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення”, здійснюється у спосіб, встановлений ДСТУ ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT) “Електронні підписи та інфраструктури (ESI). Криптографічні пакети”, шляхом вибору криптографічних параметрів відповідно до вимог до створення та перевірки удосконалених електронних підписів, що базуються на кваліфікованих сертифікатах відкритих ключів, затверджених відповідно до частини третьої статті 17^1 Закону.
