ЗАТВЕРДЖЕНО

Наказ Міністерства цифрової трансформації України

_____2024 року № ____

**Регламент**
**роботи центрального засвідчувального органу**

## І. Загальні положення

1. Цей Регламент визначає організаційно-методологічні, технічні та технологічні умови діяльності центрального засвідчувального органу (далі – ЦЗО) під час надання ним кваліфікованих електронних довірчих послуг, порядок взаємодії кваліфікованих надавачів електронних довірчих послуг (далі – надавачі) та користувачів електронних довірчих послуг з ЦЗО, а також внесення юридичних осіб та фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку.

2. Цей Регламент є обов'язковим для юридичних осіб та фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, а також надавачів та користувачів електронних довірчих послуг.

3. Цей Регламент не поширюється на надання електронних довірчих послуг відповідно до положень абзацу другого частини першої статті 2 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (далі – Закон).

4. У цьому Регламенті терміни вживаються в таких значеннях:

адміністратор інформаційно-комунікаційної системи ЦЗО (далі – Адміністратор ІКС ЦЗО) – державне підприємство «ДІЯ» (далі – ДП «ДІЯ»), яке належить до сфери управління центрального органу виконавчої влади, що забезпечує формування та реалізує державну політику у сферах електронної ідентифікації та електронних довірчих послуг, та здійснює технічне й технологічне забезпечення виконання функцій ЦЗО;

політика сертифіката ЦЗО – перелік усіх правил, що застосовуються Адміністратором ІКС ЦЗО у процесі надання електронних довірчих послуг;

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

програмно-технічний комплекс (далі – ПТК) ІКС ЦЗО – це апаратно-програмні та програмні засоби, що забезпечують виконання функцій ЦЗО згідно з вимогами до умов експлуатації та за місцезнаходженням, що зазначені в документах, отриманих за результатами впровадження заходів із захисту інформації з підтвердженою відповідністю з дотриманням положень статті 8

Закону України «Про захист інформації в інформаційно-комунікаційних системах».

Інші терміни, що вживаються у цьому Регламенті, застосовуються у значеннях, передбачених нормативно-правовими актами, що регулюють відносини у сферах електронної ідентифікації та електронних довірчих послуг.

5. Центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сферах електронної ідентифікації та електронних довірчих послуг, на який покладено виконання функцій ЦЗО, є Міністерство цифрової трансформації України:

місцезнаходження (поштова адреса): вул. Ділова, 24, м. Київ, 03150;

код за ЄДРПОУ: 43220851;

телефон: (044) 207-17-39.

Адреса електронного інформаційного ресурсу ЦЗО, доступ до якого забезпечується через комунікаційні мережі загального користування цілодобово (далі – офіційний вебсайт ЦЗО): https://czo.gov.ua.

Адреса електронної пошти для офіційного листування: inbox@czo.gov.ua

6. Адміністратор ІКС ЦЗО:

місцезнаходження (поштова адреса): вул. Ділова, 24, м. Київ, 03150;

код за ЄДРПОУ: 43395033;

адреса електронної пошти технічної підтримки: support.its@czo.gov.ua.

7. Мінцифри виконує функції ЦЗО, передбачені підпунктом 20 пункту 4 Положення про Міністерство цифрової трансформації України, затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 року № 856.

8. Адміністратор ІКС ЦЗО здійснює технічне та технологічне забезпечення виконання функцій ЦЗО, передбачених статтею $7^1$ Закону.

9. Робота Мінцифри організована в одну робочу зміну з понеділка по четвер з 09:00 до 18:00, обідня перерва – з 13:00 до 13:45; у п’ятницю – з 09:00 до 16:45, обідня перерва – з 13:00 до 13:45. Заяви та документи для внесення відомостей про юридичних осіб, фізичних осіб – підприємців до Довірчого списку, у разі припинення його діяльності, приймаються та розглядаються за адресою: вул. Ділова, 24, м. Київ, 03150.

10. Робота Адміністратора ІКС ЦЗО організована в одну робочу зміну з понеділка по четвер з 09:00 до 18:00, обідня перерва – з 13:00 до 13:45; у п’ятницю – з 09:00 до 16:45, обідня перерва – з 13:00 до 13:45 (за винятком приймання заяв надавачів на блокування, скасування та поновлення їх сертифікатів ключів, що є цілодобовим). Заяви на блокування, скасування та поновлення сертифікатів ключів подаються в електронній формі з накладенням кваліфікованого електронного підпису керівника надавача або його

уповноваженого представника через програмний інтерфейс інформаційно-комунікаційної системи ЦЗО або на адресу електронної пошти: support.its@czo.gov.ua.

Документована інформація, що передається надавачем до Адміністратора ІКС ЦЗО в разі припинення його діяльності, приймається та розглядається за адресою: вул. Ділова, 24, м. Київ, 03150.

11. Цей Регламент та зміни до нього розміщуються на офіційному вебсайті ЦЗО.

12. Формати, структура та протоколи, що застосовуються під час формування сертифікатів ключів ЦЗО, формування кваліфікованих сертифікатів відкритих ключів надавачів, формування списків відкликаних сертифікатів (далі – СВС) ЦЗО мають відповідати вимогам стандартів, які передбачені переліком стандартів, що застосовуються надавачами для надання кваліфікованих електронних довірчих послуг, та стандартів, у тому числі щодо забезпечення сумісності, що затверджуються відповідно до абзацу другого частини п’ятої статті 19 Закону.

## ІІ. Перелік кваліфікованих електронних довірчих послуг, надання яких забезпечує Адміністратор ІКС ЦЗО

1. Адміністратор ІКС ЦЗО надає кваліфіковані електронні довірчі послуги надавачам з урахуванням вимог статей $7^1$ та 29 Закону.

2. Адміністратор ІКС ЦЗО надає кваліфіковану електронну довірчу послугу формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки безоплатно на підставі договору.

## ІІІ. Посадовий склад та функції найманих працівників Адміністратора ІКС ЦЗО

1. Для виконання технічних та технологічних функцій ЦЗО Адміністратор ІКС ЦЗО створює технічний підрозділ, який складається з:

посадової особи, на яку покладені обов’язки керівника технічного підрозділу;

адміністратора реєстрації;

адміністратора сертифікації;

адміністратора безпеки;

аудитора системи;

системного адміністратора.

2. Вимоги до найманих працівників Адміністратора ІКС ЦЗО, їх функції та обов'язки, а також правила генерації та зберігання особистих ключів визначаються відповідно до таких стандартів:

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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183;

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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185;

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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185;

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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185.

## IV. Політика сертифіката ЦЗО

### 1. Сфера використання кваліфікованих сертифікатів відкритих ключів ЦЗО та надавачів

1. Адміністратор ІКС ЦЗО формує кваліфікований самопідписаний сертифікат відкритого ключа електронної печатки ЦЗО (далі – самопідписаний сертифікат електронної печатки ЦЗО) з обов'язковими реквізитами (самопідписаного сертифіката електронної печатки ЦЗО) відповідно до додатка 1 до цього Регламенту, що містить відкритий ключ, відповідний йому особистий ключ ЦЗО, призначений для формування кваліфікованих сертифікатів відкритих ключів надавачів та сертифікатів, що визначають в режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів, і СВС.

Для засвідчення інформації в Довірчому списку, використовуються окремі спеціально призначені кваліфіковані сертифікати відкритого ключа електронної печатки ЦЗО, засвідчені з використанням самопідписаного сертифіката електронної печатки ЦЗО.

Використання особистих та відповідних їм відкритих ключів за іншим призначенням (сферою використання) здійснюється з урахуванням пункту 1 глави 5 цього розділу.

2. Адміністратор ІКС ЦЗО формує кваліфіковані сертифікати відкритих ключів надавачів, що містять відкриті ключі, відповідні їм особисті ключі, призначені для формування сертифікатів ключів підписувачів, створювачів електронних печаток, СВС, надання інших кваліфікованих електронних довірчих послуг, передбачених частиною третьою статті 16 Закону.

Для кожної кваліфікованої електронної довірчої послуги надавачі використовують окремий кваліфікований сертифікат відкритого ключа, сформований Адміністратором ІКС ЦЗО.

Під час розгляду заяви про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу Адміністратор ІКС ЦЗО здійснює перевірку унікальності відкритого ключа надавача в реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів. Засвідчення відкритого ключа, який не пройшов перевірку на унікальність в реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів, забороняється.

## 2. Порядок розповсюдження інформації ЦЗО

1. На офіційному вебсайті ЦЗО розповсюджується (публікується) така інформація:

електронний сервіс, призначений для створення, перевірки та підтвердження електронного підпису та електронної печатки та його відповідність вимогам статей 18 і 19 цього Закону;

Довірчий список;

реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;

сертифікати відкритих ключів ЦЗО;

СВС;

програмний інтерфейс інформаційно-комунікаційної системи ЦЗО;

рішення про внесення відомостей про кваліфікованого надавача електронних довірчих послуг до Довірчого списку;

рішення про внесення змін до Довірчого списку;

рішення про відмову у внесенні відомостей до Довірчого списку;

рішення про скасування статусу кваліфікованого надавача електронних довірчих послуг;

відомості про прийняття від надавачів на зберігання документованої інформації, сформованих кваліфікованих сертифікатів відкритих ключів, відомостей з реєстру чинних, блокованих та скасованих кваліфікованих сертифікатів відкритих ключів у разі припинення діяльності з надання кваліфікованих електронних довірчих послуг;

результати аналізу поточного стану та перспектив розвитку у сфері електронних довірчих послуг;

нормативно-правові акти, що регулюють відносини у сферах електронної ідентифікації та електронних довірчих послуг, цей Регламент, форма договору про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки та інших кваліфікованих електронних довірчих послуг;

перелік всіх засобів кваліфікованого електронного підпису чи печатки, сертифікованих органами з оцінки відповідності, акредитованими на проведення сертифікації засобів кваліфікованого електронного підпису чи печатки та переліків засобів кваліфікованого електронного підпису чи печатки, сертифікованих органами з оцінки відповідності;

перелік органів з оцінки відповідності з гіперпосиланням на реєстр акредитованих органів з оцінки відповідності, розміщений на офіційному веб-сайті національного органу України з акредитації, а також іноземних органів з оцінки відповідності, акредитованих відповідно іноземними органами з акредитації, що є підписантами багатосторонньої угоди про визнання Міжнародного форуму з акредитації та/або Європейської кооперації з акредитації (EA MLA);

інформація щодо поточної діяльності ЦЗО.

2. Публікація чинних кваліфікованих сертифікатів відкритих ключів ЦЗО та надавачів здійснюється у спосіб визначений порядком ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів, які сформовані центральним засвідчувальним органом, затвердженого відповідно до абзацу шостого частини першої статті $7^1$ Закону.

Доступ до сертифікатів ключів ЦЗО та кваліфікованих сертифікатів відкритих ключів надавачів забезпечується цілодобово.

3. Інформація щодо скасованих та блокованих кваліфікованих сертифікатів відкритих ключів надавачів публікується на офіційному вебсайті ЦЗО у вигляді повного та часткового СВС.

4. Повні та часткові СВС публікуються відповідно до 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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 16 грудня 2021 року № 512, 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» та 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», затверджених наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185. Доступ до СВС забезпечується цілодобово.

### 3. Порядок ідентифікації та автентифікації надавачів

1. Адміністратор ІКС ЦЗО здійснює ідентифікацію та перевірку обсягу цивільної правоздатності та дієздатності заявників під час формування, блокування, скасування та поновлення кваліфікованого сертифіката відкритого ключа надавача на підставі відповідної заяви надавача відповідно до вимог статті 22 Закону та у відповідності до пункту 6.2 розділу 6 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 розділу 6 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», затверджених наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185.

2. Для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки Адміністратор ІКС ЦЗО здійснює ідентифікацію та перевірку обсягу його цивільної правоздатності та дієздатності відповідно до вимог статті 22 Закону та у відповідності до пункту 6.2 розділу 6 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 розділу 6 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», затверджених наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185.

3. Ідентифікація та перевірка обсягу цивільної правоздатності та дієздатності юридичної особи здійснюється відповідно до вимог статті 22 Закону та у відповідності до пункту 6.2 розділу 6 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 розділу 6 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», затверджених наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185.

4. Ідентифікація фізичної особи та перевірка обсягу її цивільної правоздатності та дієздатності здійснюється відповідно до вимог статті 22 Закону та у відповідності до пункту 6.2 розділу 6 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 розділу 6 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», затверджених наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185.

5. Перевірка обсягів повноважень уповноваженого представника юридичної особи здійснюється у спосіб визначений порядком проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг, затвердженим відповідно до частини п’ятої статті 22 Закону.

6. Перевірка обсягів повноважень уповноваженого представника колегіального органу юридичної особи здійснюється у спосіб визначений порядком проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг, затвердженим відповідно до частини п’ятої статті 22 Закону.

7. Перевірка обсягів повноважень фізичної особи – підприємця здійснюється у спосіб визначений порядком проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг, затвердженим відповідно до частини п’ятої статті 22 Закону.

8. Ідентифікація іноземців та перевірка обсягу їх цивільної правоздатності та дієздатності здійснюється відповідно до вимог статті 22 Закону та у відповідності до пункту 6.2 розділу 6 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 розділу 6 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», затверджених наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185.

9. Механізм підтвердження володіння надавачем особистим ключем являє собою перевірку удосконаленого електронного підпису чи печатки, накладеного(-ї) на запит для формування сертифіката ключа, особистим ключем надавача за допомогою відкритого ключа, що міститься в запиті.

10. Підтвердження володіння надавачем особистим ключем здійснюється без розкриття особистого ключа.

## 4. Управління та операційний контроль

1. Функціонування фізичного середовища ПТК ІКС ЦЗО, а також процеси та регламентні процедури, що пов’язані з генерацією та зберіганням особистих ключів ЦЗО та із формуванням кваліфікованих сертифікатів для надавачів здійснюється відповідно до 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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185;

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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185;

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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185.

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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 21 червня 2016 року № 183.

2. Контроль доступу:

1) Адміністратор ІКС ЦЗО передбачає та впроваджує захист внутрішньої обчислювальної мережі від несанкціонованого доступу з боку користувачів

зовнішньої мережі (глобальних мереж), у тому числі надавачів та третіх сторін. Засоби контролю доступу до інформаційних ресурсів ЦЗО здійснюють блокування всіх мережевих протоколів та спроб доступу, що необов'язкові для функціонування ІКС ЦЗО;

2) Адміністратор ІКС ЦЗО забезпечує розмежування доступу найманих працівників до ресурсів системи та надання функцій згідно з їхньою авторизацією так, щоб наймані працівники виконували лише ті функції, що доступні та асоційовані з їх функціями та завданнями;

3) наймані працівники повинні бути успішно ідентифіковані та автентифіковані перед початком виконання процедур, пов'язаних із формуванням сертифіката ключа або зміною його статусу;

4) всі дії найманих працівників, пов'язані з генерацією пар ключів, формуванням сертифікатів відкритих ключів або зміною їх статусу, протоколюються із забезпеченням захисту протоколів від несанкціонованого доступу;

5) резервні копії сертифікатів відкритих ключів та журналів аудиту подій зберігаються в окремому приміщенні Адміністратора ІКС ЦЗО із забезпеченням їх захисту від несанкціонованого доступу;

6) всі дії найманих працівників в ПТК ІКС ЦЗО повинні реєструватись;

7) журнали аудиту подій повинні мати захист від несанкціонованого доступу, модифікації або знищення (руйнування) інформації.

3. Процедурний контроль:

1) посадові особи, на яких покладені обов'язки керівника технічного підрозділу, адміністратора реєстрації, адміністратора сертифікації, адміністратора безпеки, аудитора системи, системного адміністратора, забезпечують належне виконання своїх обов'язків, нерозголошення конфіденційної інформації, зокрема відомостей про персональні дані надавачів, згідно із Законом;

2) інші обов'язки посадових осіб, зокрема обов'язки керівника технічного підрозділу, адміністратора реєстрації, адміністратора сертифікації, адміністратора безпеки, аудитора системи, системного адміністратора, визначаються розпорядчими документами Адміністратора ІКС ЦЗО та документами, отриманими за результатами впровадження заходів із захисту інформації з підтвердженою відповідністю з дотриманням положень статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах».

4. Ведення журналів аудиту подій:

1) у журналах аудиту подій ІКС ЦЗО реєструються дії та події таких типів:

спроби створення, знищення, встановлення паролів, зміни прав доступу в ІКС ЦЗО тощо;

заміна технічних засобів ІКС ЦЗО та пар ключів;

формування, блокування, скасування та поновлення сертифікатів ключів, формування всіх СВС;

спроби несанкціонованого доступу до ІКС ЦЗО;

надання доступу персоналу до ІКС ЦЗО;

зміна системних конфігурацій та технічне обслуговування ІКС ЦЗО;

збої в роботі ІКС ЦЗО;

інші події, відомості про які фіксуються в журналі аудиту подій ІКС ЦЗО;

2) усі записи в журналах аудиту подій в електронній або паперовій формі повинні містити дату та час дії або події, а також ідентифікувати працівника Адміністратора ІКС ЦЗО, що її здійснив або ініціював.

Аудитор системи забезпечує належне ведення журналів аудиту подій, що реєструють технічні засоби ІКС ЦЗО;

3) журнали аудиту подій підлягають перегляду не рідше одного разу на тиждень. Перегляд передбачає перевірку журналу аудиту подій на предмет несанкціонованих модифікацій, вивчення всіх дій та/або подій у журналі аудиту подій зі зверненням особливої уваги на повідомлення про невідповідності та попередження про небезпечні ситуації.

Перегляд журналів аудиту подій ІКС ЦЗО здійснює адміністратор безпеки та аудитор системи. Результати перегляду аудитор системи фіксує у відповідному журналі;

4) система ведення електронного журналу аудиту подій має бути синхронізована із Всесвітнім координованим часом із точністю до секунди та містити механізми його захисту від неавторизованого перегляду, модифікації та знищення.

Журнали аудиту подій в електронній формі резервуються з періодичністю не менше одного разу на тиждень;

5) Адміністратор ІКС ЦЗО зберігає журнали аудиту подій на місці їх створення протягом терміну, визначеному відповідно до нормативно-правових актів та пунктів 7.9 та 7.10 розділу 7 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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 р. № 185, після чого забезпечує їх передавання для архівного зберігання.

5. Ведення архівів ЦЗО:

1) архівування інформації здійснюється згідно із внутрішніми організаційно-розпорядчими документами Адміністратора ІКС ЦЗО;

2) обов'язковому архівуванню підлягають:

сертифікати відкритих ключів ЦЗО та відповідні списки відкликаних сертифікатів;

кваліфіковані сертифікати відкритих ключів надавачів;

запити на формування сертифікатів відкритих ключів в електронній формі;

журнали аудиту подій ІКС ЦЗО;

документована інформація – документи на папері та в електронній формі, що були надані надавачами Адміністратору ІКС ЦЗО, на підставі яких Адміністратором ЦЗО були надані кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані кваліфіковані сертифікати відкритих ключів для надавачів (договори, довіреності, заяви та запити на формування кваліфікованих сертифікатів), а також документи, на підставі яких Адміністратором ІКС ЦЗО були внесені відомості про надавачів та послуги, що ними надаються, до Довірчого списку;

документована інформація (документи на папері та в електронній формі), що була передана надавачами до ЦЗО в разі припинення його діяльності з надання кваліфікованих електронних довірчих послуг;

3) документи на папері та в електронній формі мають зберігатися в порядку, встановленому законодавством у сфері архівної справи;

4) знищення архівних документів має здійснюватися комісією, до складу якої входять керівник Адміністратора ІКС ЦЗО, адміністратор сертифікації, адміністратор безпеки та аудитор системи. Після завершення процедури знищення архівних документів складається відповідний акт, який затверджує керівник Адміністратора ІКС ЦЗО;

5) сертифікати відкритих ключів ЦЗО, сертифікати відкритих ключів серверів ЦЗО та сертифікати відкритих ключів адміністраторів, кваліфіковані сертифікати відкритих ключів надавачів, а також СВС зберігаються постійно;

6) для зберігання носіїв із резервними та архівними копіями виділяється окреме сховище (сейф чи відсік сейфа) з двома екземплярами ключів і пристроями для опечатування. Один екземпляр ключа від сховища знаходиться в адміністратора безпеки, другий в опечатаному вигляді зберігається у сховищі (сейфі) керівника СЗІ ІКС ЦЗО;

7) засоби, що входять до складу центрального сервера ПТК ІКС ЦЗО, забезпечують автоматичне резервне копіювання сертифікатів відкритих ключів. Автоматичне створення резервної копії має виконуватися не рідше одного разу на тиждень під час найменшого завантаження центрального сервера;

8) додатково може виконуватися резервне копіювання сертифікатів відкритих ключів на оптичні носії або інші з'ємні носії інформації в ручному режимі. Після створення нової резервної копії попередня стає архівною;

9) відновлення сертифікатів відкритих ключів із резервної копії здійснюється засобами центрального сервера шляхом зчитування сертифікатів відкритих ключів з останньої (актуальної) резервної копії та запису їх у базу даних сервера;

10) з'ємні носії зберігаються в конвертах чи упаковках, що опечатуються печаткою адміністратора сертифікації. Водночас на упаковці зазначається обліковий номер копії. Факти створення та використання копій фіксуються в окремому журналі;

11) резервні копії баз даних та журнали аудиту подій ІКС ЦЗО зберігаються у приміщенні Адміністратора ІКС ЦЗО 10 років. Контроль за здійсненням автоматичного резервного копіювання та виконання резервного копіювання в ручному режимі покладаються на системного адміністратора. Адміністратор безпеки періодично контролює процес створення та зберігання резервних копій;

12) архівне приміщення обладнується технічними засобами, які виключають можливість проникнення сторонніх осіб та неконтрольованого доступу до інформації, що підлягає архівуванню;

13) надавач, що засвідчив свій відкритий ключ у ЦЗО, у разі припинення діяльності з надання послуг здійснює передачу документованої інформації до ЦЗО;

14) механізм обов'язкового передання на зберігання ЦЗО сертифікатів ключів, документованої інформації надавачем у разі припинення його діяльності з надання послуг, а також забезпечення передавання її на архівне зберігання визначаються порядком зберігання документованої інформації та її передавання до центрального засвідчувального органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг, затвердженим відповідно до частини десятої статті 31 Закону.

## 5. Управління парами ключів ЦЗО

1. В ІКС ЦЗО використовуються особисті та відповідні їм відкриті ключі з параметрами, що відповідають вимогам стандартів з переліку стандартів, визначеного Кабінетом Міністрів України, та за такими призначеннями (сферою використання) стандартам, які визначені переліком стандартів, що застосовуються кваліфікованими надавачами електронних довірчих послуг для надання кваліфікованих електронних довірчих послуг:

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на кваліфікованих сертифікатах відкритих ключів надавачів, сертифікатів, що визначають в режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС зі ступенем розширення основного поля еліптичної кривої не менше 431 за ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий

підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі – ДСТУ 4145-2002), з функцією гешування за ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования» або за ДСТУ 7564-2014 «Інформаційні технології. Криптографічний захист інформації. Функція ґешування», затвердженим наказом Міністерства економічного розвитку і торгівлі України від 02 грудня 2014 року № 1435;

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на Довірчому списку зі ступенем розширення основного поля еліптичної кривої не менше 257 за ДСТУ 4145-2002;

особисті та відповідні їм відкриті ключі шлюзів захисту мережевих з'єднань та шифраторів мережевого потоку зі ступенем розширення основного поля еліптичної кривої не менше 257 за ДСТУ 4145-2002;

особисті та відповідні їм відкриті ключі адміністраторів, що використовуються для криптографічного захисту мережевих з'єднань, зі ступенем розширення основного поля еліптичної кривої не менше 257 за ДСТУ 4145-2002;

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на кваліфікованих сертифікатах відкритих ключів надавачів, сертифікатів, що визначають в режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС із використанням іменованої еліптичної кривої NIST P-256 (secp256r1) для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT) «Електронні підписи та інфраструктури (ESI). Криптографічні пакети», затвердженим наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 29 листопада 2022 року № 232 (далі – ДСТУ ETSI TS 119 312:2022);

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на кваліфікованих сертифікатах відкритих ключів надавачів, сертифікатів, що визначають в режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів СВС із довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI TS 119 312:2022;

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки електронної печатки ЦЗО на Довірчому списку з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI TS 119 312:2022.

2. Процедури генерації особистих та відповідних їм відкритих ключів, що використовуються в ІКС ЦЗО, створення резервних копій, відновлення з резервних копій, використання та знищення особистих ключів, що використовуються в ІКС ЦЗО, здійснюються відповідно до підпунктів 6.5.1 та

6.5.3 пункту 6.5 розділу 6 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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 08 вересня 2022 року № 185.

3. Після генерації особистих та відкритих ключів ЦЗО здійснюється формування відповідних сертифікатів ключів.

4. Строки дії особистих ключів ЦЗО відповідають строкам чинності сертифікатів відповідних їм відкритих ключів і становлять:

для особистих ключів ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів надавачів та СВС – не більше 10 років;

для особистих ключів ЦЗО для накладення електронної печатки ЦЗО на дані про статус кваліфікованих сертифікатів відкритих ключів надавачів, що визначається в режимі реального часу, – не більше 5 років;

для особистих ключів ЦЗО для накладення електронної печатки ЦЗО на Довірчому списку – не більше 10 років;

для особистих ключів шлюзу захисту мережевих з’єднань – не більше 2 років;

для особистих ключів адміністраторів – не більше 2 років.

5. Планова заміна особистого та відповідного йому відкритого ключа ЦЗО виконується на підставі окремого наказу Мінцифри.

6. Під час планової заміни особистого та відповідного йому відкритого ключа ЦЗО адміністратором сертифікації та адміністратором безпеки відповідно до вимог пунктів 2-5 цієї глави здійснюється генерація нового особистого та відповідного йому відкритого ключа ЦЗО, формування відповідного сертифіката відкритого ключа та створення резервних копій особистого ключа.

7. Після введення в дію нового особистого та відповідного йому відкритого ключа ЦЗО особистий ключ, який належить до пари ключів, для якої завершився термін дії сертифіката відкритого ключа, та всі його резервні копії знищуються способом, що унеможливлює їх відновлення, за участю адміністратора сертифікації та адміністратора безпеки.

8. Позапланова заміна особистого та відповідного йому відкритого ключа ЦЗО здійснюється в разі компрометації, підозри на компрометацію особистого ключа ЦЗО та/або особистого ключа одного з адміністраторів, а також у випадках правонаступництва, передбачених частиною десятою статті 30 Закону.

9. Під час позапланової заміни особистого та відповідного йому відкритого ключа ЦЗО адміністратором сертифікації та адміністратором безпеки відповідно

до вимог пунктів 2-5 цієї глави здійснюються генерація нового особистого та відповідного йому відкритого ключа ЦЗО, формування відповідного сертифіката відкритого ключа та створення резервних копій особистого ключа.

10. У разі підтвердження факту компрометації особистих ключів ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів, сертифікати, що визначають в режимі реального часу статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС, усі попередньо сформовані кваліфіковані сертифікати відкритих ключів надавачів, сертифікати, що визначають в режимі реального часу статус кваліфікованих сертифікатів відкритих ключів надавачів та сертифікат ключа для перевірки електронної печатки ЦЗО скасовуються та формується СВС, який підписується з використанням нового особистого ключа ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів надавачів, сертифікати, що визначають в режимі реального часу статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС.

11. Усі особисті ключі ЦЗО та особисті ключі адміністраторів, факт компрометації яких було підтверджено, знищуються способом, що унеможливлює їх відновлення, за участю двох адміністраторів, у тому числі адміністратора безпеки.

12. Факти знищення особистих ключів ЦЗО, особистих ключів адміністраторів та їх резервних копій реєструються адміністратором безпеки у відповідному журналі обліку.

13. Не пізніше завершення половини строку дії поточного особистого та відповідного йому відкритого ключів ЦЗО для накладення та перевірки електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів надавачів, сертифікати, що визначають в режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС здійснюються генерація нового особистого та відповідного йому відкритого ключа ЦЗО для накладення та перевірки електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів надавачів, сертифікати, що визначають в режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС та формування відповідного сертифіката ключа. Водночас поточний особистий ключ ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів надавачів, сертифікати, що визначають в режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС стає попереднім, а новий – поточним.

14. Адміністратор ІКС ЦЗО інформує надавачів та контролюючий орган про здійснення планової та невідкладно – про здійснення позапланової заміни особистих та відкритих ключів ЦЗО.

## 6. Забезпечення захисту особистого ключа ЦЗО

1. Особисті ключі ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів, сертифікати, що визначають в

режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС, особисті ключі ЦЗО для накладення електронної печатки ЦЗО на Довірчому списку, розміщуються в засобі кваліфікованого електронного підпису чи печатки, що є апаратно-програмним або апаратним пристроєм, за допомогою якого здійснювалася генерація пари ключів.

2. Для зберігання особистих ключів шлюзів захисту мережевих з'єднань, шифраторів мережевого потоку та особистих ключів адміністраторів застосовують лише засоби кваліфікованого електронного підпису чи печатки, які відповідають вимогам, встановленим частинами першою та другою статті 19 Закону.

3. Поточні особисті ключі ЦЗО для накладення електронної печатки ЦЗО на кваліфікованих сертифікатах відкритих ключів надавачів, сертифікати, що визначають в режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС мають зберігатися в засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями і входять до складу ІКС ЦЗО, та використовуватися для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів надавачів, сертифікати, що визначають в режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС.

4. Попередні особисті ключі ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів, сертифікати, що визначають в режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС мають розміщуватися в засобі кваліфікованого електронного підпису чи печатки, що є апаратно-програмним або апаратним пристроєм, за допомогою якого здійснювалася генерація пари ключів, та використовуватися для обслуговування кваліфікованих сертифікатів відкритих ключів надавачів, які були сформовані за допомогою цих ключів.

5. Передавання особистих ключів ЦЗО, особистих ключів шлюзів захисту мережевих з'єднань та шифраторів мережевого потоку здійснюється за актом приймання-передавання ключів.

Забороняється:

передавання особистих ключів адміністраторів між адміністраторами;

виносити особисті ключі ЦЗО та їх резервні копії зі спеціального приміщення ІКС ЦЗО.

6. Резервне копіювання та відновлення особистих ключів ЦЗО здійснюються адміністратором сертифікації під контролем адміністратора безпеки.

7. Для забезпечення можливості відновлення особистого ключа ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів, сертифікати, що визначають в режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС, особистого ключа ЦЗО для накладення електронної печатки ЦЗО на Довірчий список, в разі

виходу з ладу засобів кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, виконується резервне копіювання відповідного особистого ключа з такого засобу лише на засоби кваліфікованого електронного підпису чи печатки, які відповідають вимогам, встановленим частинами першою та другою статті 19 Закону.

8. Для забезпечення можливості відновлення особистих ключів шлюзів захисту мережевих з'єднань, шифраторів мережевого потоку та особистих ключів адміністраторів у разі виходу з ладу засобу кваліфікованого електронного підпису чи печатки виконується резервне копіювання особистого ключа з цих засобів на окремі резервні засоби кваліфікованого електронного підпису чи печатки, які відповідають вимогам, встановленим частинами першою та другою статті 19 Закону.

9. Факти генерації та створення резервних копій особистого ключа ЦЗО для накладення електронної печатки ЦЗО на кваліфіковані сертифікати відкритих ключів, сертифікати, що визначають в режимі реального часу, статус кваліфікованих сертифікатів відкритих ключів надавачів та СВС, особистого ключа ЦЗО для накладення електронної печатки ЦЗО на Довірчий список, особистих ключів шлюзів захисту мережевих з'єднань, особистих ключів шифраторів мережевого потоку, особистих ключів адміністраторів та відповідних їм відкритих ключів реєструються адміністратором безпеки у відповідному журналі обліку.

10. Технічні специфікації форматів, які реалізуються в засобах кваліфікованого електронного підпису чи печатки, встановлюються головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах електронної ідентифікації та електронних довірчих послуг, спільно зі спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

## V. Положення сертифікаційних практик ЦЗО

### 1. Подання запиту на формування кваліфікованого сертифіката відкритого ключа та надання сформованого кваліфікованого сертифіката відкритого ключа надавачу

1. Адміністратор ІКС ЦЗО формує кваліфіковані сертифікати відкритих ключів юридичних осіб або фізичних осіб – підприємців, що мають намір надавати кваліфіковані електронні довірчі послуги, надавачам, які відповідають вимогам, встановленим частинами першою та другою статті 23 Закону, та забезпечує цілодобовий доступ до інформації про дату та час зміни статусу кваліфікованих сертифікатів відкритих ключів.

2. Формування кваліфікованого сертифіката відкритого ключа надавача здійснюється на підставі заяви про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого

сертифіката електронного підпису чи печатки кваліфікованому надавачу електронних довірчих послуг – юридичній особі (додаток 2 до цього Регламенту) та заяви про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки кваліфікованому надавачу електронних довірчих послуг – фізичній особі – підприємцю (додаток 3 до цього Регламенту), що подаються до Адміністратора ІКС ЦЗО.

3. Заява про формування кваліфікованого сертифіката відкритого ключа подається до Адміністратора ІКС ЦЗО в електронній формі.

Заява в електронній формі, на яку накладається кваліфікований електронний підпис керівника юридичної особи, фізичної особи – підприємця чи їх уповноваженого представника, надсилається через програмний інтерфейс інформаційно-комунікаційної системи або на електронну пошту Адміністратора ІКС ЦЗО: support.its@czo.gov.ua.

4. Разом із заявою про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надсилаються на електронну пошту Адміністратора ІКС ЦЗО підписані кваліфікованим електронним підписом керівника юридичної особи, фізичною особою – підприємцем чи їх уповноваженим представником такі документи:

запит на формування сертифіката;

договір про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки.

5. Вимоги до запиту:

запит подається у форматі згідно зі специфікацією синтаксису запиту на сертифікацію (PKCS#10), що визначена RFC 2986 «PKCS #10: CertificationRequestSyntaxSpecification»;

запит має містити інформацію про відкритий ключ надавача, що подає такий запит. Зазначена інформація визначається атрибутом «Інформація про відкритий ключ надавача» (subjectPublicKeyInfo), формат якого має відповідати стандартами, у тому числі щодо забезпечення сумісності, перелік яких затверджується відповідно до абзацу другого частини п’ятої статті 19 Закону.

Запит, крім обов’язкових реквізитів (кваліфікованого надавача електронних довірчих послуг в запиті на формування сертифіката ключа), що визначені додатком 1 до цього Регламенту, та послуг надавача, може містити інші ідентифікаційні дані фізичних або юридичних осіб, необов’язкові додаткові спеціальні атрибути, визначені у стандартах для кваліфікованих сертифікатів відкритих ключів. Ці атрибути не мають впливати на інтероперабельність і визнання кваліфікованих електронних підписів.

6. Розгляд заяви про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу становить не більше п’яти робочих днів від дати прийняття заяви.

Під час розгляду заяви про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу здійснюється перевірка:

відповідності даних, внесених до заяви, документам надавача, отриманим від Мінцифри відповідно до встановленого порядку ведення Довірчого списку;

унікальності відкритого ключа послуги за відомостями реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

належності надавачу відповідного особистого ключа послуги шляхом перевірки удосконаленого електронного підпису чи печатки в запиті;

відповідності запиту вимогам, зазначеним у пункті 5 цієї глави.

7. У разі успішної перевірки Адміністратор ІКС ЦЗО формує кваліфікований сертифікат відкритого ключа надавача. У разі непроходження перевірки у строк, передбачений абзацом першим пункту 6 цієї глави, надавачу надається вмотивована відмова у формуванні сертифіката ключа та повертається заява про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу разом із додатками до неї.

8. Формування кваліфікованих сертифікатів відкритих ключів надавачів здійснюється адміністратором сертифікації під контролем адміністратора безпеки.

9. Під час формування кваліфікованого сертифіката відкритого ключа додаткові розширення, що можуть міститись у запиті, встановлюються у кваліфікованому сертифікаті відкритого ключа надавача за умови, що вони були визначені як не критичні, а об’єктні ідентифікатори таких розширень зареєстровані у встановленому порядку.

10. Після формування кваліфікованого сертифіката відкритого ключа надавача Адміністратор ІКС ЦЗО надсилає на електронну пошту надавача, зазначену в Довірчому списку та в реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів, документи в електронній формі, на які накладено кваліфікований електронний підпис уповноваженого представника Адміністратора ІКС ЦЗО, а саме:

сформований(ні) кваліфікований(ні) сертифікат(и) надавача;

акт наданих послуг (для кожного з сертифікатів) про формування кваліфікованого сертифіката;

договір про надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки надавачу.

## 2. Умови використання кваліфікованих сертифікатів відкритих ключів та особистих ключів надавачів

1. Надавачі використовують пари ключів (особистих та відкритих) за призначенням (сферою використання) згідно з 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», затвердженим наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 16 грудня 2021 року № 512.

2. Під час надання послуг надавачі повинні використовувати пари ключів (особистих та відкритих) із такими параметрами:

зі ступенем розширення основного поля еліптичної кривої не менше 257 за ДСТУ 4145-2002;

зі ступенем розширення основного поля еліптичної кривої не менше 256 для алгоритму ECDSA за ДСТУ ETSI TS 119 312:2022;

з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI TS 119 312:2022.

3. Для обчислення значення геш-функції використовуються алгоритми, визначені відповідно до 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», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 16 грудня 2021 року № 512.

ДСТУ 4145-2002 застосовується з функцією гешування за ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования» або за ДСТУ 7564-2014 «Інформаційні технології. Криптографічний захист інформації. Функція ґешування», затвердженим наказом Міністерства економічного розвитку і торгівлі України від 02 грудня 2014 року № 1435.

Алгоритми ECDSA та RSA застосовуються з функціями гешування відповідно до ДСТУ ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT) «Електронні підписи та інфраструктури (ESI). Криптографічні пакети», затвердженого наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 29 листопада 2022 року № 232.

4. Надавачі використовують особисті ключі тільки за призначенням (сферою використання) в період чинності відповідних кваліфікованих сертифікатів

відкритих ключів, сформованих відповідно до цього Регламенту, та за умови, що цей сертифікат не був заблокований або скасований.

5. Надавачі забезпечують використання кваліфікованих сертифікатів відкритих ключів та особистих ключів, зазначених у пункті 2 глави 1 розділу IV цього Регламенту, тільки за призначенням (сферою використання).

6. Під час надання кваліфікованих електронних довірчих послуг надавачі забезпечують обов'язковість перевірки строку чинності та статусу сформованих Адміністратором ЦЗО сертифікатів відкритих ключів.

7. Перед використанням будь-якого сертифіката відкритого ключа має забезпечуватись перевірка:

чинності кваліфікованого сертифіката відкритого ключа надавача на момент накладення кваліфікованого електронного підпису чи створення електронної печатки на документ або кваліфікованого електронного підпису чи печатки на документі;

чинності кваліфікованої електронної печатки ЦЗО, що була додана до кваліфікованого сертифіката відкритого ключа надавача за допомогою самопідписаного сертифіката ключа ЦЗО, чинного на момент формування кваліфікованого сертифіката відкритого ключа надавача;

статусу кваліфікованого сертифіката відкритого ключа надавача в режимі реального часу, якщо перевірка здійснюється на момент чинності цього сертифіката ключа або за СВС.

8. Під час перевірки статусу кваліфікованого сертифіката відкритого ключа надавача за СВС здійснюється перевірка автентичності, цілісності та терміну дії СВС.

## 3. Обставини та порядок зміни статусу (скасування, блокування, поновлення) кваліфікованого сертифіката відкритого ключа

1. Скасування кваліфікованого сертифіката відкритого ключа надавача:

1) скасування кваліфікованих сертифікатів відкритих ключів надавачів здійснюється у випадках, передбачених частинами першою – третьою статті 25 Закону, за надходженням інформації або на підставі заяви про скасування кваліфікованого сертифіката відкритого ключа надавача;

2) форми заяви про скасування кваліфікованого сертифіката відкритого ключа кваліфікованого надавача електронних довірчих послуг – юридичної особи (додаток 4 до цього Регламенту) та заяви про скасування кваліфікованого сертифіката відкритого ключа кваліфікованого надавача електронних довірчих послуг – фізичної особи – підприємця (додаток 5 до цього Регламенту) подаються до Адміністратора ІКС ЦЗО;

3) заява про скасування кваліфікованого сертифіката відкритого ключа подається надавачем до Адміністратора ІКС ЦЗО в електронній формі, на яку

накладено кваліфікований електронний підпис керівника юридичної особи, фізичної особи – підприємця чи їх уповноваженого представника або в будь-який інший спосіб, що забезпечує підтвердження особи – надавача відповідно до вимог законодавства;

4) під час приймання заяви про скасування кваліфікованого сертифіката відкритого ключа здійснюється встановлення особи керівника юридичної особи – надавача (фізичної особи – підприємця, що є надавачем) або їх уповноваженого представника та перевіряється достатність обсягу цивільної правоздатності та дієздатності шляхом перевірки ідентифікаційних даних особи з документів, що надаються заявником, та даних, одержаних з інформаційних систем органів державної влади;

5) не приймаються до розгляду заяви та документи, якщо кваліфікований електронний підпис не пройшов перевірку;

6) опрацювання заяви на скасування кваліфікованого сертифіката відкритого ключа та інформування Адміністратором ІКС ЦЗО надавача про скасування сертифіката ключа його послуги здійснюються протягом двох годин від моменту отримання заяви Адміністратором ІКС ЦЗО;

7) скасування кваліфікованого сертифіката відкритого ключа надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки;

8) скасування кваліфікованого сертифіката відкритого ключа надавача набирає чинності з дати та часу здійснення цієї операції;

9) серійний номер скасованого кваліфікованого сертифіката відкритого ключа надавача вноситься до СВС із зазначенням дати та часу здійснення цієї операції.

2. Блокування кваліфікованого сертифіката відкритого ключа надавача:

1) блокування кваліфікованих сертифікатів відкритих ключів надавачів здійснюється у випадках, передбачених частинами шостою та сьомою статті 25 Закону, на підставі заяви про блокування кваліфікованого сертифіката відкритого ключа кваліфікованого надавача електронних довірчих послуг – юридичної особи (додаток 6 до цього Регламенту) та заяви про блокування кваліфікованого сертифіката відкритого ключа для кваліфікованого надавача електронних довірчих послуг – фізичної особи – підприємця (додаток 7 до цього Регламенту), що подаються до Адміністратора ІКС ЦЗО, або у разі повідомлення контролюючим органом про підозру в компрометації особистого ключа користувача електронних довірчих послуг, набрання законної сили рішенням суду про блокування кваліфікованого сертифіката відкритого ключа;

2) заява про блокування кваліфікованого сертифіката відкритого ключа подається надавачем до Адміністратора ІКС ЦЗО в електронній формі з накладенням кваліфікованого електронного підпису керівника юридичної особи, фізичної особи – підприємця чи їх уповноваженого представника;

3) під час приймання заяви про блокування кваліфікованого сертифіката відкритого ключа здійснюється ідентифікація керівника юридичної особи – надавача (фізичної особи – підприємця, що є надавачем) або їх уповноваженого представника відповідно до вимог статті 22 Закону та перевіряється обсяг його повноважень у спосіб визначений порядком проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця під час надання електронних довірчих послуг, затвердженим відповідно до частини п’ятої статті 22 Закону;

4) не приймаються до розгляду заяви про блокування, якщо кваліфікований електронний підпис не пройшов перевірку;

5) кваліфікований сертифікат відкритого ключа надавача блокується не пізніше ніж протягом двох годин від моменту отримання заяви про блокування кваліфікованого сертифіката відкритого ключа Адміністратором ІКС ЦЗО;

6) блокування кваліфікованого сертифіката відкритого ключа надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки;

7) блокування кваліфікованого сертифіката відкритого ключа надавача набирає чинності з дати та часу здійснення цієї операції;

8) серійний номер заблокованого кваліфікованого сертифіката відкритого ключа надавача вноситься до СВС із зазначенням дати та часу здійснення цієї операції.

3. Поновлення кваліфікованого сертифіката відкритого ключа надавача:

1) поновлення кваліфікованих сертифікатів відкритих ключів надавачів здійснюється у випадках, передбачених частинами десятою, одинадцятою статті 25 Закону, на підставі заяви про поновлення кваліфікованого сертифіката відкритого ключа кваліфікованого надавача електронних довірчих послуг – юридичної особи (додаток 8 до цього Регламенту) та заяви про поновлення кваліфікованого сертифіката відкритого ключа кваліфікованого надавача електронних довірчих послуг – фізичної особи – підприємця (додаток 9 до цього Регламенту), або надходженням інформації до Адміністратора ІКС ЦЗО у інший спосіб, встановлений Законом;

2) заява про поновлення кваліфікованого сертифіката відкритого ключа подається до Адміністратора ІКС ЦЗО в електронній формі з накладенням кваліфікованого електронного підпису керівника юридичної особи, фізичної особи – підприємця чи їх уповноваженого представника;

3) під час приймання заяви про поновлення кваліфікованого сертифіката відкритого ключа здійснюється ідентифікація керівника юридичної особи – надавача (фізичної особи – підприємця, що є надавачем) або їх уповноваженого представника відповідно до вимог статті 22 Закону та перевіряється обсяг його повноважень у спосіб, визначений порядком проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця

під час надання електронних довірчих послуг, затвердженим відповідно до частини п’ятої статті 22 Закону;

4) не приймаються до розгляду заяви про поновлення, якщо кваліфікований електронний підпис не пройшов перевірку;

5) заблокований кваліфікований сертифікат відкритого ключа надавача поновлюється не пізніше ніж протягом двох годин від моменту отримання заяви про поновлення кваліфікованого сертифіката відкритого ключа Адміністратором ІКС ЦЗО;

6) поновлення кваліфікованого сертифіката відкритого ключа надавача здійснюється адміністратором сертифікації під контролем адміністратора безпеки;

7) поновлення кваліфікованого сертифіката відкритого ключа надавача набирає чинності з дати та часу здійснення цієї операції;

8) відомості щодо поновлення кваліфікованого сертифіката відкритого ключа надавача вносяться до СВС із зазначенням дати та часу здійснення цієї операції.

4. Розповсюдження інформації про зміну статусу кваліфікованих сертифікатів відкритих ключів надавачів:

1) розповсюдження інформації про статус кваліфікованих сертифікатів відкритих ключів надавачів здійснюється за допомогою публікації повного та часткового СВС на офіційному вебсайті ЦЗО та забезпечення можливості перевірки статусу сертифіката ключа в режимі реального часу через електронні комунікаційні мережі загального користування;

2) публікація наступного СВС здійснюється з періодичністю, зазначеною у пункті 4 глави 2 розділу IV цього Регламенту;

3) Адміністратор ІКС ЦЗО під час формування СВС забезпечує такі умови:

у кожному СВС зазначається граничний термін його дії до видання наступного списку;

новий СВС може бути опублікований до настання граничного терміну його дії для видання наступного списку;

на СВС має бути накладена електронна печатка ЦЗО;

4) інформація про статус кваліфікованого сертифіката відкритого ключа надавача в режимі реального часу розповсюджується за протоколом визначення статусу сертифіката відповідно до вимог стандартів, передбачених переліком стандартів, що застосовуються кваліфікованими надавачами електронних довірчих послуг для надання кваліфікованих електронних довірчих послуг, та стандартів, у тому числі щодо забезпечення сумісності, що затверджуються відповідно до абзацу другого частини п’ятої статті 19 Закону.

### 4. Закінчення строку чинності кваліфікованого сертифіката відкритого ключа надавача

1. Строк чинності кваліфікованого сертифіката відкритого ключа надавача становить не більше ніж п’ять років.

2. Початок строку чинності кваліфікованого сертифіката відкритого ключа надавача обчислюється з дати та часу формування сертифіката у ЦЗО, що відображається в сертифікаті.

3. Не пізніше закінчення половини строку чинності кваліфікованого сертифіката відкритого ключа надавача останній отримує новий кваліфікований сертифікат відкритого ключа в порядку, визначеному у пунктах 1-8 глави 1 розділу V цього Регламенту.

## VI. Надання адміністративної послуги із внесення відомостей про юридичних осіб та фізичних осіб – підприємців, які мають намір надавати кваліфіковані електронні довірчі послуги, до Довірчого списку

1. Надання адміністративної послуги внесення юридичних осіб та фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку, внесення змін до Довірчого списку здійснюється Мінцифри з урахуванням положень Закону та Закону України «Про адміністративні послуги».

2. На адміністративну послугу внесення юридичних осіб та фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку, внесення змін до Довірчого списку Мінцифри затверджуються інформаційна і технологічна картки.

3. Інформаційна картка розміщується в місці здійснення приймання юридичних осіб та фізичних осіб – підприємців, які мають намір надавати електронні довірчі послуги, на офіційному вебсайті ЦЗО та Єдиному державному вебпорталі електронних послуг.

4. Порядок подання юридичною особою або фізичною особою – підприємцем, що має намір надавати послуги, документів та їх розгляд ЦЗО передбачений частиною другою статті 30 Закону, а також набуття статусу або скасування статусу надавача здійснюється відповідно до статті 30 Закону.

5. Внесення відомостей до Довірчого списку, внесення змін, скасування статусу кваліфікованого надавача електронних довірчих послуг здійснюються у спосіб визначений порядком ведення Довірчого списку, затвердженим центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сферах електронної ідентифікації та електронних довірчих послуг відповідно до частини десятої статті 30 Закону.

6. Форми заяви про внесення до Довірчого списку юридичної особи та заяви про внесення до Довірчого списку фізичної особи – підприємця передбачені відповідно додатком 10 та додатком 11 до цього Регламенту.

7. Форми заяви про внесення змін до Довірчого списку у зв’язку зі зміною відомостей та заяви про внесення змін до Довірчого списку щодо внесення нової кваліфікованої електронної довірчої послуги передбачені відповідно додатком 12 та додатком 13 до цього Регламенту.

**Директор директорату**
**розвитку цифровізації** **Анастасія ХАЛЄЄВА**