ПОГОДЖЕНО

Державна служба спеціального
зв'язку та захисту інформації України

Заступник Голови Служби

_____ **О.В. Потій**

«25» 03 2021 р.

ЗАТВЕРДЖЕНО

Товариство з обмеженою
відповідальністю «ІЛАЙФ»

Директор

_____ **Є.І. Лук'янчук**

«03» 03 2021 р.

РЕГЛАМЕНТ
РОБОТИ КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ ТОВАРИСТВА З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ІЛАЙФ»

На 42 аркушах

2021

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Регламент роботи ТОВ «Ілайф» (далі – Регламент) є нормативним документом, що визначає організаційно- методологічні та технологічні умови діяльності кваліфікованого надавача електронних довірчих послуг (далі – КНЕДП, Надавач) ТОВ «Ілайф», під час надання кваліфікованих електронних довірчих послуг (далі – довірчі послуги).

Регламент визначає порядок та процедури обслуговування кваліфікованих сертифікатів відкритих ключів (далі – сертифікат, сертифікат ключа) користувачів кваліфікованих електронних довірчих послуг (далі – КЕДП), умови надання послуг та правил користування КЕДП, а також основні організаційно-технічні заходи, що направлені на забезпечення функціонування КНЕДП.

Регламент розроблено відповідно до чинного законодавства України у сфері електронних довірчих послуг:

- Закону України від 05 жовтня 2017 року № 2155-VIII “Про електронні довірчі послуги” (далі – Закон);
- Закону України від 22 травня 2003 року № 851 - IV “Про електронні документи та електронний документообіг” (зі змінами);
- Закону України від 15 травня 2003 року № 755 - IV “Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань”;
- Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07 листопада 2018 року № 992 (далі – Вимоги);
- Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затверджених постановою Кабінету Міністрів України від 19.09.2018 № 749.
- інших нормативно-правових актів у сфері надання електронних довірчих послуг. Норми цього Регламенту поширюються на:
  - працівників надавача;
  - заявників;
  - підписувачів;
  - створювачів електронної печатки.

Цей Регламент є обов’язковим для заявників та підписувачів (фізичних осіб та фізичних осіб – представників органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій незалежно від їх організаційно-правової форми та форми власності) та є засобом офіційного повідомлення та інформування всіх сторін у взаєминах, що виникають у процесі надання кваліфікованих електронних довірчих послуг.

Визнання вимог цього Регламенту користувачами електронних довірчих послуг є обов’язковою умовою та підставою для укладання з ними договору про надання кваліфікованих електронних довірчих послуг.

Вимоги Регламенту засновані на принципах дотримання прав та виконання обов’язків суб’єктами надання та отримання кваліфікованих довірчих послуг, які наведено в Законі України «Про електронні довірчі послуги».

У цьому Регламенті терміни вживаються в такому значенні:

відокремлений пункт реєстрації – представництво (філія, підрозділ, територіальний орган) надавача електронних довірчих послуг або юридична чи фізична особа, яка на підставі наказу надавача електронних довірчих послуг (його керівника) або договору, укладеного з ним, здійснює реєстрацію заявників на отримання кваліфікованих електронних довірчих послуг з дотриманням вимог Закону «Про електронні довірчі послуги» та законодавства у сфері захисту інформації;

відповідальні працівники надавача – обслуговуючий персонал надавача та відокремленого пункту реєстрації, обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг;

договір – окремий договір, відповідно до якого надаються кваліфіковані електронні довірчі послуги;

захищений засіб особистих ключів– засіб кваліфікованого електронного підпису чи печатки, що призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на ньому даних від несанкціонованого доступу, безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання (далі по тексту - НКІ);

заявник – фізична особа, фізична особа - представник юридичної особи, що звернулася до надавача для отримання кваліфікованих електронних довірчих послуг;

користувачі – підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних, інші фізичні та юридичні особи, які отримують електронні довірчі послуги у надавачів таких послуг;

програмно-технічний комплекс надавача – апаратні, апаратно-програмні та програмні засоби, що забезпечують виконання функцій, пов'язаних із наданням електронних довірчих послуг;

підписувач – фізична особа, фізична особа - представник юридичної особи яка створює електронний підпис;

створювач електронної печатки – юридична особа, яка створює електронну печатку;

уповноважений представник юридичної особи – відповідальний підрозділ або працівник, що забезпечує організацію використання кваліфікованих електронних довірчих послуг в установі.

Інші терміни застосовуються у значеннях, наведених у Законі України від 05.10.2017 № 2155-VIII «Про електронні довірчі послуги» (далі – Закон), Вимогах у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07.11.2018 № 992 (далі – Вимоги), Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затверджених постановою Кабінету Міністрів України від 19.09.2018 № 749 (далі – Порядок), інших нормативно-правових актах з питань криптографічного та технічного захисту інформації.

Положення цього Регламенту поширюються в електронній формі шляхом розміщення на офіційному електронному інформаційному ресурсі надавача з врахуванням вимог пункту 43 Вимог.

Ідентифікаційні дані надавача:

Повне найменування організації: Товариство з обмеженою відповідальністю «Ілайф»;

Скорочене найменування організації: ТОВ «Ілайф»;

місцезнаходження (поштова адреса): 04119, Київ, вул. Глибочицька, буд. 17, корп. 2, літ. А, оф. 328;

код за ЄДРПОУ: 36049014;

телефони: +38 067 325 91 15;

адреса офіційного електронного інформаційного ресурсу:

https://ca.e-life.com.ua;

електронна пошта: ca@e-life.com.ua.

Представництвами надавача є відокремлені пункти реєстрації, що представлені окремими підрозділами або позаштатними одиницями ТОВ «Ілайф», відряджені до певного регіону, для надання електронних довірчих послуг, посадові особи (адміністратори реєстрації) або юридичні чи фізичні особи, які на підставі договору/угоди/довіреності з ТОВ «Ілайф», здійснюють реєстрацію підписувачів з дотриманням вимог законодавства у сфері електронних довірчих послуг та захисту інформації.

Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені ТОВ «Ілайф».

Робота надавача організована в одну робочу зміну з понеділка по четвер з 9:00 до 18:00, обідня перерва – з 13:00 до 13:45; у п’ятницю – з 9:00 до 16:45, обідня перерва – з 13:00 до 13:45.

Діяльність надавача щодо прийому запитів на блокування, скасування та поновлення кваліфікованих сертифікатів відкритих ключів є цілодобовою.

Вимоги до процедур з управління ризиками, персоналом, операційною безпекою, інцидентами, доказами та архівами, поводження з персональними даними користувачів, процедур встановлення заявника та відокремлених пунктів реєстрації визначаються цим Регламентом та організаційно-розпорядчою документацією надавача.

Внесення змін та доповнень до цього Регламенту, погодження та затвердження змін та доповнень здійснюється відповідно до пункту 42 Вимог.

У разі внесення змін до Регламенту, надавач інформує про це шляхом розміщення відповідних змін на офіційному електронному інформаційному ресурсі надавача.

Зміни та доповнення до Регламенту, що не пов'язані зі зміною чинного законодавства України, набувають чинності через 10 календарних днів з дня розміщення зазначених змін і доповнень на офіційному веб-сайті надавача.

Всі зміни та доповнення, що внесені до Регламенту у зв’язку зі зміною законодавства, набувають чинності одночасно зі вступом у дію відповідних нормативно-правових актів.

Якщо підписувач не погоджується із внесеними до Регламенту змінами та доповненнями, він має право припинити використання сертифіката.

2. ПЕРЕЛІК КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

Надавач забезпечує надання таких кваліфікованих електронних довірчих послуг:

- кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки;

- кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;
- кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованої електронної позначки часу.

3. ПЕРЕЛІК ПОСАД ТА ФУНКЦІЇ НАЙМАНИХ ПРАЦІВНИКІВ

Працівниками надавача, посадові обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг, є працівники ТОВ «Ілайф» за штатним розкладом та/або за трудовим договором, на яких покладено функціональні обов'язки:

- керівника КНЕДП;
- адміністратора реєстрації;
- адміністратора сертифікації;
- адміністратора безпеки та аудиту;
- системного адміністратора.

Керівник (начальник) КНЕДП відповідає за керування профільним підрозділом, вчасне та якісне виконання покладених на нього функціональних завдань. В межах виконання своїх обов'язків відповідає за організацію та контроль процесів, направлених на забезпечення функціонування, розвитку надавача та захист інформації в інформаційно-телекомунікаційній системі (далі – ІТС) Надавача, а саме:

- контроль за виконанням регламентних процедур з експлуатації та технічного обслуговування ІТС Надавача;
- контроль за впровадженням та забезпеченням функціонування комплексної системи захисту інформації ІТС Надавача;
- контроль за забезпеченням працездатності загальносистемного та спеціального програмного ІТС Надавача;
- забезпечення актуалізації баз даних, створюваних та оброблюваних в ІТС Надавача;
- розгляд та оцінка технічних рішень щодо модернізації ІТС Надавача;
- розробка та узгодження технічних завдань, проектної та експлуатаційної документації ІТС Надавача та комплексної системи захисту інформації ІТС Надавача;
- контроль за будівельно-монтажними та пусконалагоджувальними роботами;
- проведення попередніх випробувань, дослідної експлуатації та введення ІТС Надавача в експлуатацію.

Адміністратор реєстрації: роль адміністратора, яка надає працівникові повноваження щодо створення облікових записів заявника в рамках порталу ІТС, створення та контролю заявок про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів та реалізації функцій працівників надавача, посадові обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг (адміністратор реєстрації) згідно з п. 10, 11 «Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України» від 07.11.2018 № 992.

Основними обов’язками адміністратора реєстрації є:

- ідентифікація та автентифікація заявників;
- перевірка заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів;
- встановлення належності відкритого ключа та відповідного йому особистого ключа заявнику;
- ведення обліку користувачів;
- надання допомоги під час генерації пари ключів підписувача або створювача електронної печатки;
- надання консультацій щодо умов та порядку отримання кваліфікованих електронних довірчих послуг.

Адміністратор сертифікації: роль адміністратора, яка надає працівникові повноваження для формування кваліфікованих сертифікатів відкритих ключів, ведення електронного реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів, збереження та використання особистих ключів надавача, створення їх резервних копій та реалізації функцій працівників надавача, посадові обов’язки яких безпосередньо пов’язані з наданням кваліфікованих електронних довірчих послуг (адміністратор сертифікації) згідно з п. 12, 13«Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України» від 07.11.2018 № 992..

Основними обов’язками адміністратора сертифікації є:

- участь у генерації пар ключів надавача та створенні резервних копій особистих ключів надавача;
- зберігання особистих ключів надавача та їх резервних копій;
- забезпечення використання особистих ключів надавача під час формування та обслуговування кваліфікованих сертифікатів відкритих ключів надавача та користувачів;
- участь у знищенні особистих ключів надавача;
- забезпечення ведення, архівування та відновлення баз даних кваліфікованих сертифікатів відкритих ключів користувачів;
- забезпечення публікації кваліфікованих сертифікатів відкритих ключів користувачів та списків відкликаних сертифікатів на офіційному веб-сайті надавача;
- створення резервних копій кваліфікованих сертифікатів відкритих ключів користувачів;
- зберігання кваліфікованих сертифікатів відкритих ключів користувачів, їх резервних копій, списків відкликаних сертифікатів та інших важливих ресурсів інформаційно-телекомунікаційної системи надавача.

Адміністратор безпеки та аудиту: роль адміністратора, яка надає працівникові повноваження щодо створення/видалення/налаштування облікових записів користувачів, перегляду журналів реєстрації подій та налаштування політик аудиту ПЗ та реалізації функцій працівників надавача, посадові обов’язки яких безпосередньо пов’язані з наданням кваліфікованих електронних довірчих послуг (адміністратор безпеки та аудиту) згідно з п. 14-16 «Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України» від 07.11.2018 № 992.

Основними обов’язками адміністратора безпеки та аудиту є:

- участь у генерації пар ключів надавача та створенні резервних копій особистих ключів надавача;

- контроль за формуванням, обслуговуванням і створенням резервних копій кваліфікованих сертифікатів відкритих ключів надавача, користувачів та списків відкликаних сертифікатів;
- контроль за зберіганням особистих ключів надавача та їх резервних копій, особистих ключів посадових осіб;
- участь у знищенні особистих ключів надавача, контроль за правильним і своєчасним знищенням посадовими особами їх особистих ключів;
- організація розмежування доступу до ресурсів інформаційно-телекомунікаційної системи надавача;
- забезпечення спостереження за функціонуванням комплексної системи захисту інформації або системи управління інформаційною безпекою (реєстрація подій в інформаційно-телекомунікаційній системі надавача, моніторинг подій тощо);
- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації або системи управління інформаційною безпекою після збоїв, відмов, аварій інформаційно-телекомунікаційної системи надавача;
- забезпечення режиму доступу до приміщень надавача, в яких розміщена інформаційно-телекомунікаційна система надавача;
- ведення журналів обліку адміністратора безпеки та аудиту, визначених документацією щодо комплексної системи захисту інформації або звітності, що передбачена системою управління інформаційною безпекою;
- проведення перевірок журналів аудиту подій, що реєструють технічні засоби інформаційно-телекомунікаційної системи надавача;
- проведення перевірок відповідності положень внутрішньої організаційно-розпорядчої документації надавача та документації щодо комплексної системи захисту інформації або системи управління інформаційною безпекою;
- контроль за дотриманням найманими працівниками надавача положень внутрішньої організаційно-розпорядчої документації надавача та документації щодо комплексної системи захисту інформації або системи управління інформаційною безпекою;
- контроль за веденням баз даних надавача;
- контроль за веденням архіву надавача.

Адміністратор безпеки та аудиту відповідає за проведення перевірок дотримання найманими працівниками надавача положень внутрішньої організаційно-розпорядчої документації надавача та документації щодо комплексної системи захисту інформації або системи управління інформаційною безпекою.

Забороняється суміщення посадових обов’язків адміністратора безпеки та аудиту з іншими посадовими обов’язками, безпосередньо пов’язаними з наданням кваліфікованих електронних довірчих послуг.

Надавач повинен мати щонайменше дві посади адміністратора безпеки та аудиту.

Системний адміністратор: роль адміністратора, яка надає працівникові повноваження щодо адміністрування ПЗ, виконання процедур технологічного обслуговування (оновлення, резервне копіювання, відкат конфігурації тощо) та реалізації функцій працівників надавача, посадові обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг (системний адміністратор) згідно з п. 17, 18 «Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України» від 07.11.2018 № 992.

Основними обов'язками системного адміністратора є:

- організація експлуатації та технічного обслуговування ІТС надавача і адміністрування її технічних засобів;
- забезпечення функціонування офіційного веб-сайту надавача;
- участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації;
- ведення журналів аудиту подій, що реєструють технічні засоби інформаційно-телекомунікаційної системи надавача;
- встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення інформаційно-телекомунікаційної системи надавача;
- встановлення та налагодження штатної підсистеми резервного копіювання бази даних інформаційно-телекомунікаційної системи надавача;
- забезпечення актуалізації баз даних, створюваних та оброблюваних в інформаційно-телекомунікаційній системі надавача, у зв'язку із збоями.

До складу працівників відокремлених пунктів реєстрації Надавача входять наймані працівники надавача або працівники юридичних осіб та фізичні особи, які на підставі договору (угода, довіреність) з надавачем здійснюють реєстрацію заявників з дотриманням вимог законодавства у сфері захисту інформації та електронних довірчих послуг.

На працівників відокремлених пунктів реєстрації покладено функціональні обов'язки:

- віддаленого адміністратора реєстрації;
- адміністратора безпеки та аудиту на відокремленому пункті реєстрації.

Віддалений адміністратор реєстрації відповідає за виконання функцій та несе обов'язки адміністратора реєстрації, визначені у цьому регламенті, в рамках відповідного віддаленого пункту реєстрації.

В межах виконання своїх обов'язків адміністратор безпеки та аудиту на відокремленому пункті реєстрації відповідає за належну експлуатацію комплексу засобів захисту відокремленого пункту реєстрації, проведення перевірок дотримання найманими працівниками надавача положень внутрішньої організаційно-розпорядчої документації надавача та документації щодо комплексної системи захисту інформації або системи управління інформаційною безпекою, контроль за роботою програмного забезпечення відокремленого пункту реєстрації, контроль за використанням особистих ключів персоналу відокремленого пункту реєстрації.

4. ПОЛІТИКА СЕРТИФІКАТА ТА ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

4.1 Політика сертифіката

4.1.1 Перелік сфер, в яких дозволяється використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем

Кваліфіковані сертифікати відкритих ключів Надавача формуються Адміністратором інформаційно-телекомунікаційної системи Центрального засвідчувального органу (далі – Адміністратор ІТС ЦЗО) та містять відкриті ключі, відповідні яким особисті ключі, які призначені для формування сертифікатів ключів підписувачів чи створювачів електронних печаток, списків відкликаних сертифікатів, надання інших кваліфікованих електронних довірчих послуг, передбачених частиною другою статті 16 Закону.

Для кожної кваліфікованої електронної довірчої послуги надавач використовує окремий кваліфікований сертифікат відкритого ключа.

Надавач формує кваліфіковані сертифікати відкритих ключів підписувачів, створювачів електронних печаток, відповідно до вимог частини другої статті 23 Закону.

Кваліфіковані сертифікати відкритих ключів, сформовані Надавачем, дозволено використовувати для:

- автентифікації;
- перевірки кваліфікованого електронного підпису;
- перевірки кваліфікованої електронної печатки;
- узгодження ключів шифрування.

Для ідентифікації сфери використання відкритих ключів, під час формування кваліфікованого сертифіката відкритого ключа надавач встановлює розширення сертифіката "Призначення відкритого ключа" ("keyUsage"), зазначені у таблиці 4.1:

Таблиця 4.1

Сфера використання кваліфікованого сертифіката відкритого ключа	Призначення відкритого ключа ("keyUsage")
Автентифікація	digitalSignature + nonRepudiation або keyAgreement
Перевірка кваліфікованого електронного підпису	digitalSignature + nonRepudiation
Перевірка кваліфікованої електронної печатки	digitalSignature + nonRepudiation
Узгодження ключів шифрування	keyAgreement

Надавач формує кваліфіковані сертифікати відкритого ключа з розширеннями сертифіката digitalSignature + nonRepudiation або keyAgreement за умови, що такі відкриті ключі належать до різних ключових пар.

Для сфери перевірки кваліфікованої електронної печатки під час формування кваліфікованого сертифіката відкритого ключа надавач встановлює додаткове розширення “Уточнене призначення відкритого ключа” “extendedKeyUsage” із об’єктним ідентифікатором 1.2.804.2.1.1.1.3.9. В сертифікатах електронних печаток юридичних осіб, призначених для

використання в програмних реєстраторах розрахункових операцій відповідно до Закону України №128-IX «Про внесення змін до Закону України "Про застосування реєстраторів розрахункових операцій у сфері торгівлі, громадського харчування та послуг" та інших законів України щодо детінізації розрахунків у сфері торгівлі та послуг», додатково вказується ознака «Для РРО № Х», де Х – номер реєстратора розрахункових операцій.

4.1.2 Обмеження щодо використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем

Обмеження щодо використання сформованих надавачем сертифікатів ключів застосовуються у відповідності до положень цього Регламенту та діючого законодавства України.

Інформація щодо обмеження сфери використання сертифіката ключа заноситься до сформованого сертифіката ключа у вигляді уточненого призначення ключа.

Не допускається використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем для певної сфери використання, в інших сферах.

4.1.3 Перелік інформації, що розміщується надавачем на офіційному веб-сайті

До інформації, вільний доступ до якої забезпечує надавач через офіційний веб-сайт, належать:

- відомості про надавача;
- дані про внесення відомостей про надавача до Довірчого списку;
- Регламент роботи надавача;
- кваліфіковані сертифікати відкритих ключів надавача;
- перелік кваліфікованих електронних довірчих послуг, які надає надавач;
- дані про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг;
- форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;
- реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;
- відомості про обмеження під час використання кваліфікованих сертифікатів відкритих ключів користувачами;
- дані про порядок перевірки чинності кваліфікованого сертифіката відкритого ключа, у тому числі умови перевірки статусу кваліфікованого сертифіката відкритого ключа; − перелік актів законодавства у сфері електронних довірчих послуг;
- відомості про відокремлені пункти реєстрації, у разі їх наявності(адреса, графік роботи, контакти); відомості про виїзного реєстратора (ПІБ, посада, повноваження, фото, тощо);

Надавач також забезпечує інформування користувачів про умови отримання кваліфікованих електронних довірчих послуг шляхом розміщення відповідної інформації на офіційному веб-сайті надавача.

Інформація, що публікується на електронному інформаційному ресурсі надавача, є загальнодоступною.

4.1.4 Час і порядок публікації кваліфікованих сертифікатів відкритих ключів та списків відкликаних сертифікатів

Кваліфіковані сертифікати відкритих ключів Надавача публікуються одразу після їх отримання від Центрального засвідчувального органу.

Кваліфіковані сертифікати відкритих ключів серверів ІТС Надавача публікуються одразу після їх формування Надавачем.

Кваліфіковані сертифікати відкритих ключів підписувачів та створювачів електронної печатки, які надали згоду на їх публікацію, публікуються одразу після формування таких сертифікатів.

Надавач формує списки відкликаних сертифікатів у вигляді повного та часткового списків, які відповідають таким вимогам:

- у кожному списку відкликаних сертифікатів зазначається граничний строк його дії до видання нового списку;
- новий список відкликаних сертифікатів може бути опубліковано до настання граничного строку його дії до видання наступного списку;
- на список відкликаних сертифікатів повинен бути накладений кваліфікований електронний підпис надавача.

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

Час зміни статусу кваліфікованих сертифікатів відкритих ключів синхронізований із Всесвітнім координованим часом (UTC) з точністю до однієї секунди.

Посилання на списки відкликаних сертифікатів вносяться до кваліфікованих сертифікатів відкритих ключів підписувачів та створювачів електронної печатки.

Повний список відкликаних сертифікатів формується та публікується 1 раз на тиждень та містить інформацію про всі відкликані сертифікати ключів, які були сформовані надавачем.

Частковий список відкликаних сертифікатів формується та публікується кожні 2 години і містить інформацію про всі відкликані кваліфіковані сертифікати, статус яких був змінений в інтервалі між часом випуску останнього повного списку відкликаних сертифікатів та часом формування поточного часткового списку відкликаних сертифікатів.

У випадку одночасного використання надавачем декількох діючих особистих ключів і відповідних до них сертифікатів надавач може вести декілька списків відкликаних сертифікатів, підписаних різними особистими ключами. В такому разі всі вони публікуються на веб-сайті надавача у наведеному вище порядку.

4.1.5 Механізм підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа

Відкритий ключ заявника надається для формування кваліфікованого сертифіката відкритого ключа виключно у вигляді самопідписаного запиту формату PKCS#10. Підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа, забезпечується шляхом перевірки удосконаленого електронного підпису, створеного за допомогою особистого ключа заявника на запиті на

формування кваліфікованого сертифіката, за допомогою відкритого ключа, що міститься у цьому запиті, або під час генерації пари ключів одразу після ідентифікації заявника, за умови його особистої присутності.

Підтвердження володіння заявником особистим ключем здійснюється без розкриття особистого ключа.

4.1.6 Умови встановлення (ідентифікації) заявника

Відповідно до Статті 22 Закону України «Про електронні довірчі послуги» під час формування та видачі кваліфікованого сертифіката відкритого ключа надавач здійснює встановлення (ідентифікацію) особи.

Формування та видача кваліфікованого сертифіката відкритого ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті відкритого ключа, не допускаються.

Ідентифікація фізичної особи, яка вперше звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, здійснюється за умови її особистої присутності за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про ЄДДР та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

Допускається ідентифікація заявника кваліфікованим надавачем електронних довірчих послуг за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката.

Ідентифікація іноземців здійснюється відповідно до законодавства за умови наявності у заявника посвідки на проживання та національного паспорта іноземця або документа, що його замінює.

Під час перевірки цивільної правоздатності та дієздатності юридичної особи кваліфікований надавач електронних довірчих послуг зобов’язаний ознайомитися з інформацією про юридичну особу, що міститься в ЄДР, а також пересвідчитися, що обсяг її цивільної правоздатності та дієздатності є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа.

Встановлення особи-заявника повинно відбуватись з використанням наявних сервісів перевірки чинності документів та ідентифікаційної інформації про особу. До таких сервісів можуть належати сервіси "Перевірка за базою недійсних документів" (nd.dmsu.gov.ua) та "Єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань" (usr.minjust.gov.ua).

Кваліфікований надавач електронних довірчих послуг під час формування та видачі кваліфікованого сертифіката відкритого ключа здійснює ідентифікацію особи уповноваженого представника юридичної особи відповідно до вимог Закону України «Про електронні довірчі послуги», а також перевіряє обсяг його повноважень за документом або за даними з ЄДР, що визначають повноваження представника.

Якщо від імені юридичної особи діє колегіальний орган, кваліфікованому надавачу електронних довірчих послуг подається документ, у якому визначено повноваження відповідного органу та розподіл обов’язків між його членами.

До розгляду не приймаються документи/копії документів, які мають підчистки, дописки,

закреслені слова, інші виправлення або мають пошкодження, внаслідок чого їх текст (фото) неможливо прочитати (розпізнати).

Для ідентифікації особи заявника, що звернувся до надавача для отримання кваліфікованих електронних довірчих послуг, надавач вимагає разом із заявою надати, а заявник надає ідентифікаційні дані, які вносяться до кваліфікованого сертифіката відкритого ключа.

Після позитивної ідентифікації адміністратор реєстрації приймає рішення про реєстрацію заявника.

Реєстрація здійснюється за особистої присутності заявника та є підставою для формування відповідних кваліфікованих сертифікатів відкритих ключів.

Для реєстрації заявника – юридичної особи уповноважений представник юридичної особи надає такі документи:

- підписаний договір - у двох примірниках або заповнену та підписану заявником картку приєднання до договору - в одному примірнику;
- оригінал довідки, виписки чи витягу з ЄДР, або копію цього документу, засвідчену нотаріально або підписом керівника та печаткою юридичної особи (за наявності);
- копії паспортів заявників або інших документів, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи, засвідчені відповідними заявниками або нотаріально; для ідентифікації особи заявник має надати для звірки оригінал паспорту;
- копії довідок про присвоєння ідентифікаційних номерів (карток фізичних осіб – платників податку) заявників, засвідчені відповідними заявниками або нотаріально (у випадку, якщо наданий паспорт підписувача не містить значення ІН або копії сторінок паспорту у разі відмови від отримання ідентифікаційного номеру платника податків); для ідентифікації особи заявник має надати для звірки оригінал ідентифікаційного номеру платника податків;
- оригінали або засвідчені копії документів, що підтверджують належність заявника до юридтчної особи та його повноваження;
- заява на формування кваліфікованих сертифікатів, засвідчені відповідними заявниками (встановлена форма заявки на формування сертифіката розміщена на інформаційному ресурсі надавача).

Оригінал виписки або витягу з ЄДР може бути наданий в електронному вигляді відповідно до чинного законодавства.

Для реєстрації заявника – ФОП/фізичної особи надаються такі документи:

- підписаний договір - у двох примірниках або заповнену та підписану картку приєднання до договору - в одному примірнику;
- копія паспорта заявника або інших документів, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний

демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи, засвідчені відповідними заявниками або нотаріально; для ідентифікації особи заявник має надати для звірки оригінал паспорту;

- копія довідки про присвоєння ідентифікаційного номера (картки фізичної особи – платника податку), засвідчена підписувачем або нотаріально (у випадку, якщо наданий паспорт підписувача не містить значення ІН або копії сторінок паспорту у разі відмови від отримання ідентифікаційного номеру платника податків); для ідентифікації особи заявник має надати для звірки оригінал ідентифікаційного номеру платника податків;
- заява на формування кваліфікованих сертифікатів, засвідчені відповідними заявниками (встановлена форма заявки на формування сертифіката розміщена на інформаційному ресурсі надавача).

Переліки, форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги, та роз'яснення щодо їх оформлення публікуються на офіційному веб-сайті надавача.

Для укладання договорів про надання кваліфікованих електронних довірчих послуг надавач може отримувати від заявників інші документи, передбачені законодавством.

Для підтвердження належного проведення процедури встановлення заявника, надавач забезпечує зберігання заяв на формування або зміну статусу кваліфікованих сертифікатів відкритих ключів та копій документів, які надавались заявниками під час ідентифікації. Копії таких документів зберігаються в паперовому вигляді в архівних приміщенням надавача або відокремлених пунктів реєстрації надавача, а також в електронному вигляді із забезпеченням захисту інформації відповідно до вимог нормативних документів у сфері захисту інформації, автоматичного резервного копіювання засобами ІТС надавача та ручного архівного копіювання на окремі носії інформації.

Заяви та копії документів, які використовувались в процедурі встановлення заявника, засвідчуються за правилами, наведеними у Таблиці 4.1.

Таблиця 4.1

Форма документа	**Засвідчення з боку заявника**		**Засвідчення з боку надавача (адміністратора реєстрації)**	
	Тип підпису	**Черга засвідчення**	**Тип підпису**	**Черга засвідчення**
Паперова	Власноручний підпис	Перша	Штамп адміністратора реєстрації на паперових документах Кваліфікований електронний підпис адміністратора реєстрації в підсистемі створення облікових записів користувачів	Друга

Електронна	Кваліфікований електронний підпис або електронний підпис, отриманий за допомогою засобів відтворення власноручного підпису з використанням інтерактивних сенсорних дисплеїв	Перша	Кваліфікований електронний підпис адміністратора реєстрації на електронному документі Кваліфікований електронний підпис адміністратора реєстрації в підсистемі створення облікових записів користувачів	Друга

Засвідчення надавачем заяв та копій документів без завершення встановлення особи заявника та без належного засвідчення ним документів не допускається.

Оригінал виписки або витягу з ЄДР може бути наданий в електронному вигляді відповідно до чинного законодавства.

Під час встановлення особи надавач може використовувати засоби фотофіксації факту пред'явлення заявником документів, що посвідчують особу. Збереження фотодокументів в ІТС надавача здійснюється після їх засвідчення шляхом створення кваліфікованого електронного підпису адміністратора реєстрації з дотриманням вимог законодавства щодо захисту персональних даних.та захисту інформації.

4.1.7 Механізм автентифікації користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований надавачем

Автентифікація користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований надавачем, здійснюється у випадку подання в електронній формі заяв про формування, блокування та скасування кваліфікованих сертифікатів відкритих ключів, у разі незмінності ідентифікаційних даних внесених до попереднього кваліфікованого сертифіката відкритого ключа з моменту формування сертифіката до моменту створення кваліфікованого електронного підпису на заяві.

Перевірка ідентифікаційних даних заявника, який звертається з заявою в електронній формі, а також законності такого звернення, здійснюється шляхом автентифікації заявника та його повноважень за результатами перевірки кваліфікованого електронного підпису на заяві та встановленням чинності на момент подання заяви сертифіката ключа, що містить ідентифікаційні дані особи.

4.1.8 Механізми автентифікації користувачів під час блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа

Перелік та опис механізмів автентифікації користувачів під час звернень щодо блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа наведено у таблиці 4.2.

Таблиця 4.2

Тип операції (причина подання заяв)	Форма подання заяв	Механізми підтвердження ідентифікаційних даних
Блокування кваліфікованого сертифіката відкритого ключа	Усна	За ключовою фразою голосової автентифікації, первинний обмін якою між користувачем та надавачем здійснюється під час подання заяви про формування кваліфікованого сертифіката відкритого ключа
	Письмова паперова	Аналогічні механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа
	Письмова електронна	Аналогічні механізмам підтвердження ідентифікаційних даних користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований надавачем
Скасування кваліфікованого сертифіката відкритого ключа	Письмова паперова	Аналогічні механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа
	Письмова електронна	Аналогічні механізмам підтвердження ідентифікаційних даних користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований надавачем
Поновлення кваліфікованого сертифіката відкритого ключа	Письмова паперова	Методами підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа

4.1.9 Опис фізичного середовища

Приміщення надавача розділені на функціональні зони за рівнями безпеки, встановленими відповідно до Вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 14.05.2020 № 269, зареєстрованим в Мінюсті 16.07.2020 за № 668/34951.

Усі засоби ПТК ІТС Надавача розташовуються в приміщеннях будівель, контроль за доступом до яких здійснюється силами державної та іншої охорони та відповідальним персоналом в межах встановлених повноважень.

Приміщення відповідають вимогам техніки безпеки та протипожежної безпеки, комплектуються необхідними засобами енергозабезпечення, охоронної та протипожежної

сигналізації, відеоспостереження (за необхідності), допоміжними технічними засобами (у робочому приміщенні КНЕДП – механічний (електронний) замок; у кімнаті реєстрації КНЕДП – механічний (електронний) замок; у спеціальному приміщенні КНЕДП: перші двері – механічний замок, другі двері – спеціальний замок із запором, системами життєзабезпечення (кондиціонерами).

Спеціальне приміщення КНЕДП відповідає вимогам до спеціальних приміщень, у тому числі вимогам щодо захисту від витоку та деструктивного впливу зовнішніх електромагнітних полів, а ПТК, який використовується для обслуговування сертифікатів користувачів, має експертний висновок в галузі криптографічного захисту інформації та відповідає вимогам нормативних документів в сфері технічного захисту інформації стосовно створення комплексної системи захисту інформації.

Для кожного рівня безпеки приміщень на підставі оцінених ризиків та відповідних цим ризикам обраних механізмів їх нейтралізації визначено вимоги до необхідного набору механізмів безпеки, зокрема: контролю доступу, виявлення вторгнень, пожежної сигналізації та пожежогасіння, альтернативних та резервних джерел електроживлення тощо (далі – механізми безпеки приміщень). Вимоги мають бути визначені в рамках Положення про експлуатацію ІТС Надавача.

4.1.9.1 Фізичне розташування ПТК обладнання ЦОД ІТС Надавача

Комутаційне обладнання та серверні компоненти, що використовуються в складі ЦОД ІТС Надавача розміщені в окремій машинній залі на базі реалізації інформаційно-телекомунікаційної системи хмарного центру обробки даних ТОВ «Анте Медіам» (далі – ІТС ХЦОД), із забезпеченням належного рівня фізичного захисту доступу персоналу ТОВ «Анте Медіам» та працездатності обладнання системи, що підтверджуєтеся атестатом відповідності №15631 від 25 вересня 2017 року.

ІТС ЦОД знаходиться в приміщеннях на цокольному поверсі адміністративної будівлі за адресою: м. Київ, вул. Паркова дорога, 16А. Вхід на територію приміщення, де знаходяться серверні і мережеві компоненти ІТС ХЦОД та робочі місця адміністраторів, наданий тільки уповноваженому персоналу, який визначений розпорядчими документами ТОВ «Анте Медіам» та обмежений для сторонніх осіб.

Програмно-технічний комплекс та засоби кваліфікованого електронного підпису чи печатки розміщені в окремій машинній залі ТОВ «Анте Медіам», із забезпеченням розмежування доступу персоналу ТОВ «Анте Медіам» та надавача електронних довірчих послуг та працездатності обладнання системи.

Компоненти ЦОД ІТС Надавача розташовуються ТОВ «Анте Медіам» в окремих приміщеннях, які обладнані системою фізичного обмеження доступу, системою відеоспостереження, системою пожежогасіння та системою кондиціонування/вентиляції. Компоненти розміщені на контрольованій території, яка охороняється, де забезпечується пропускний режим в робочий та неробочий час.

Вказані приміщення мають рівень безпеки 4 відповідно до Рекомендації Адміністрації Державної служби спеціального зв’язку та захисту інформації України до встановлення рівнів безпеки та механізмів безпеки приміщень кваліфікованого надавача електронних довірчих послуг, опублікованих на офіційному сайті Служби, також наявні Приміщення (коридори) буферної зони - рівень безпеки 3.

Фізичне розміщення визначено та зафіксовано в договорі хостингу/оренди з оператором інфраструктури ІТС ХЦОД, яким встановлено:

- Обладнання постачальника послуг «Хмарний центр обробки даних» знаходиться на території України. Адреса: Україна, м. Київ, нул. Паркова дорога, 16А.
- Будівлі обладнані системами електроживлення, опалення, кондиціювання, пожежною та охоронною сигналізацією. Трьохрівнева система охорони, що забезпечує охорону приміщень та спостерігає за охоронною сигналізацією серверної після постановки приміщень на сигналізацію.
- Температурний режим приміщень розгортання інфраструктури ІТС ХЦОД відповідає вимогам, встановленим виробником обладнання.
- Персонал забезпечує відмовостійкість апаратного обладнання датацентру без погіршення характеристик обслуговування в разі відмов окремих компонентів.
- Всі інженерні системи та обладнання дата-парку мають дублювання N+1 або 2N, що забезпечує безперебійну роботу 24Х7Х365.
- Електроживлення здійснюється з двох незалежних джерел.

Заходи забезпечення працездатності серверного та комутаційного обладнання ЦОД ІТС забезпечують рівень відмовостійкості, достатній для безпечного відключення обладнання та відновлення працездатності системи в терміни, які визначаються технологічними процесами обробки даних в ІТС Надавача (підтверджено за результатом державної експертизи).

Лінії внутрішньої комутації обладнання ЦОД розміщено на території будівлі із унеможливленням фізичного доступу.

4.1.9.2 Фізичне розташування резервного ПТК обладнання ЦОД ІТС Надавача

Комутаційне обладнання та серверні компоненти, що використовуються в складі ЦОД ІТС Надавача розміщені в окремій машинній залі на базі реалізації програмно-апаратного комплексу реалізації «Віртуального хмарного датацентру» ДЕ НОВО, із забезпеченням належного рівня фізичного захисту доступу персоналу ТОВ «Деново» та працездатності обладнання системи, що підтверджуєтеся атестатом відповідності №14162 від 22 липня 2016р.

Заходи забезпечення працездатності серверного та комутаційного обладнання ЦОД ІТС забезпечують рівень відмовостійкості, достатній для безпечного відключення обладнання та відновлення працездатності системи в терміни, які визначаються технологічними процесами обробки даних в ІТС Надавача (підтверджено за результатом державної експертизи).

Фізичне середовище реалізації «Віртуального хмарного датацентру» ДЕ НОВО включає: приміщення серверної зали розміщення програмно-апаратного комплексу реалізації інфраструктури «Хмарний центр обробки даних» ДЕ НОВО, системи та засоби забезпечення експлуатації обладнання (електроживлення, сигналізація, вентиляція, кондиціонування, пожежний захист).

Фізичне розміщення визначено та зафіксовано в договорі хостингу/оренди з оператором інфраструктури «Хмарний центр обробки даних», яким встановлено:

- Обладнання постачальника послуг «Хмарний центр обробки даних» знаходиться на території України. Адреса: Україна, м. Київ, вул. Північно-Сирецька, 1-3.
- Будівлі обладнані системами електроживлення, опалення, кондиціювання, пожежною та охоронною сигналізацією. Трирівнева система охорони, що забезпечує охорону приміщень та спостерігає за охоронною сигналізацією серверної після постановки приміщень на сигналізацію.

– Температурний режим приміщень розгортання інфраструктури «Хмарний центр обробки даних» відповідає вимогам, встановленим виробником обладнання.

– Персонал забезпечує відмовостійкість апаратного обладнання датацентру без погіршення характеристик обслуговування в разі відмов окремих компонентів.

– Всі інженерні системи та обладнання дата-парку мають дублювання N+1 або 2N, що забезпечує безперебійну роботу 24X7X365.

– Електроживлення здійснюється з двох незалежних джерел.

Лінії внутрішньої комутації обладнання ЦОД розміщено на території будівлі із унеможливленням фізичного доступу.

4.1.9.3 Фізичне розташування ПТК сегменту адміністрування ІТС Надавача

Фізичне середовище сегменту адміністрування ІТС Надавача включає приміщення ТОВ «Ілайф», системи та засоби забезпечення експлуатації обладнання ІТС (електроживлення, сигналізація, вентиляція, кондиціонування, пожежний захист) розміщені за адресою: Україна, Київ, вул. Глибочицька, буд. 17, корп. 2, літ. А, оф. 328.

Політика обмеження фізичного доступу до приміщень визначається Регламентом. Всі ділянки та приміщення ТОВ «Ілайф», де встановлено комп'ютери та інше обладнання ІТС, поділяються умовно на дві зони безпеки (третій та четвертий рівень безпеки реалізований у місці розміщення ПТК опис згідно п.4.1.9.1, 4.1.9.2 даного Регламенту):

1) Перший рівень. Офісний простір надання послуг – приміщення ТОВ «Ілайф» доступ до яких надається для співробітників організації та відвідувачів в рамках надання кваліфікованих електронних довірчих послуг та інших технологічних процесів.

2) Другий рівень. Службові приміщення - кабінети персоналу ТОВ «Ілайф», в яких розташовуються АРМ користувачів ІТС. Можливість доступу до приміщень визначається особисто власниками приміщень (відповідальними співробітниками ТОВ «Ілайф»).

Приміщення 3-го та 4-го рівнів безпеки розташовані у місці фізичного розміщення ПТК. Там же й знаходиться безпечне сховище для зберігання резервних копій КЕП. Доступ на даний рівень дозволений обмеженому колу працівників згідно з затвердженим керівництвом ТОВ «Ілайф» переліком (системний адміністратор та адміністратор безпеки й аудиту) та у встановленому порядку згідно Списку уповноважених осіб Замовника, які мають право доступу до обладнання, що розміщене в Датацентрі «Парковий» (ТОВ «Анте Медіам»), що є невід’ємним додатком до Договору.

Комплексне застосування механізмів безпеки, які взаємно доповнюють один одного, формує інтегровану електронну систему безпеки, що забезпечує безперебійну експлуатацію об’єктів і критичних систем надавача в середовищі із загальним високим рівнем безпеки.

До складу електроної системи безпеки входять такі підсистеми:

- контролю доступу (наявність цілодобової охорони приміщень (договір з орендодавцем на охорону));
- виявлення вторгнень та сигналізації (наявна охоронна сигналізація);
- відеоспостереження замкнутого контуру (наявні камери відеоспостереження);
- автоматичного виявлення пожежі та пожежогасіння (наявна система виявлення пожежі та протипожежної сигналізації).

Впроваджено організаційні заходи з контролю доступу до приміщень та обладнання («Порядок доступу в приміщення серверної»).

Температурний режим приміщень розгортання засобів відповідає вимогам встановленим виробником обладнання.

Лінії комутації обладнання рівня доступу розміщено на території закладу із унеможливленням фізичного доступу.

4.1.9.4 Умови фізичного розташування ПТК ВПР Надавача

Віддалені пункти реєстрації, які підключаються до ІТС Надавача, розглядаються як сукупність ПЕОМ, організованих у вигляді окремих віддалених автоматизованих робочих місць (далі – АРМ) користувачів в складі ЛОМ відповідних фізичних осіб-підприємців та/або юридичних організацій. Допускається використання персональних ЕОМ та мобільних ЕОМ (ноутбуків), що забезпечують підключення та взаємодію із засобами кваліфікованого електронного підпису та печатки

На віддалених технічних майданчиках реалізації ВПР не передбачається можливість зберігання будь-яких даних, всі дані, що циркулюють в ІТС, зберігаються централізовано в межах баз даних ЦОД ІТС.

Вимоги щодо забезпечення безпеки розгортання та експлуатації ПТК ВПР повинні відповідати вимогам до фізичного середовища розташування ПТК сегменту адміністрування ІТС Надавача.

Дані, що передаються між компонентами структурної схеми ІТС Надавача за допомогою загальних мереж передачі даних, передаються у зашифрованому вигляді з використанням загальних протоколів передачі даних та засобів КЗІ.

4.1.9.5 Вимоги до безпечного сховища та порядку доступу до нього

Безпечне сховище, призначене для зберігання носіїв критичної для надання послуг надавачем інформації (атрибути доступу до засобів кваліфікованого електронного підпису чи печатки, в яких зберігаються дані резервних копій особистого ключа надавача, засоби авторизації в ПТК надавача тощо), знаходиться у спеціальному приміщенні Надавача.

Конструкція сховища передбачає достатню кількість індивідуальних відсіків для кожної уповноваженої посадової особи, яка згідно з посадовими обов'язками виконує роботи з критичною для надавача інформацією.

Доступ до відсіків здійснюється за участі двох уповноважених посадових осіб Надавача, які згідно з посадовими обов'язками виконують роботи з критичною для надавача інформацією.

Безпечне сховище має сертифікат про відповідність ДСТУ EN 1143-1 "Засоби безпечного зберігання. Вимоги, класифікація та методи випробування на тривкість щодо зламування. Частина 1: Сховища, двері сховищ, сейфи та АТМ-сейфи".

4.1.10 Процедурний контроль

Недотримання найманими працівниками надавача своїх посадових обов’язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації надавача та документації комплексної системи захисту інформації передбачає дисциплінарні стягнення, адміністративну та кримінальну відповідальність, передбачені:

- трудовим договором;
- Кодексом України про адміністративні правопорушення;
- Кримінальним кодексом України.

Працівники, які виконують функції, безпосередньо пов'язані із наданням кваліфікованих електронних довірчих послуг, приступають до виконання таких функцій після ознайомлення із посадовими інструкціями.

4.1.11 Порядок ведення журналів аудиту подій

Типи подій, частота перегляду, строки зберігання журналів аудиту подій, методи захисту та резервного копіювання журналів аудиту подій, перелік найманих працівників надавача, що можуть здійснювати перегляд журналів аудиту подій наведено у Таблиці 4.3.

Таблиця 4.3

Тип події	**Частота перегляду**	**Строк зберігання**	**Форма ведення**	**Метод захисту**	**Доступ на перегляд**
Встановлення параметрів (налаштувань) операційних систем та програмного забезпечення	≤ 1 раз на тиждень	Постійно	Електронна	засобами ОС/ засобами ПЗ ІТС надавача	Адміністратор безпеки та аудиту
Встановлення прав доступу та інших параметрів безпеки	≤ 1 раз на тиждень	Постійно	Електронна	засобами ОС/ засобами ПЗ ІТС надавача	Адміністратор безпеки та аудиту
Генерація, використання та знищення ключових даних	за необхідності	Постійно	Паперова/ електронна	засобами ОС/ засобами ПЗ ІТС надавача/ зберігання у сховищах (сейфах)	Адміністратор безпеки та аудиту
Внесення, модифікація та видалення реєстраційних даних підписувачів	≤ 1 раз на добу	Постійно	Електронна	засобами ОС/ засобами ПЗ ІТС надавача	Адміністратор безпеки та аудиту

Формування, блокування, скасування та поновлення сертифікатів ключів, а також формування списків відкликаних сертифікатів	≤ 1 раз на добу	Постійно	Електронна	засобами ОС/ засобами ПЗ ІТС надавача	Адміністратор безпеки та аудиту
Створення резервних копій та відновлення реєстру сертифікатів та списків відкликаних сертифікатів та іншої важливої інформації	≤ 1 раз на добу	Постійно	Електронна	засобами ОС/засобами ПЗ ІТС надавача/ зберігання носіїв інформації у сховищах (сейфах)	Адміністратор безпеки та аудиту
Отримання персоналом доступу до автоматизованої системи надавача та її складових частин (вхід до операційної системи тощо)	≤ 1 раз на тиждень	Постійно	Електронна	засобами ОС/ засобами ПЗ ІТС надавача	Адміністратор безпеки та аудиту
Спроби несанкціонованого доступу до автоматизованої системи надавача та її складових частин	≤ 1 раз на добу	Постійно	Електронна	засобами ОС/ засобами ПЗ ІТС надавача	Адміністратор безпеки та аудиту
Збої у роботі автоматизованої системи надавача та її складових частин	≤ 1 раз на добу	Постійно	Паперова/ електронна	засобами ОС/ засобами ПЗ ІТС надавача/	Адміністратор безпеки та аудиту

Усі записи в журналах аудиту подій в електронній або паперовій формі повинні містити дату та час події, а також ідентифікаційну інформацію щодо суб'єкта, що ініціював цю подію.

4.1.12 Порядок ведення архівів надавача

Види документів та даних, що підлягають архівуванню, строки зберігання архівів, механізм та порядок зберігання і захисту архівів наведено у Таблиці 4.4.

Таблиця 4.4

Види документів та даних	Форма зберігання	Строк зберігання	Механізм зберігання
Кваліфіковані сертифікати відкритих ключів надавача	Електронна	Постійно	Автоматичне резервне копіювання засобами ІТС надавача та ручне архівне копіювання на окремі носії інформації
Кваліфіковані сертифікати відкритих ключів надавача серверів надавача (OCSP, TSP, CMP)	Електронна	Постійно	Автоматичне резервне копіювання засобами ІТС надавача та ручне архівне копіювання на окремі носії інформації
Кваліфіковані сертифікати відкритих ключів надавача адміністраторів	Електронна	Постійно	Автоматичне резервне копіювання засобами ІТС надавача та ручне архівне копіювання на окремі носії інформації
Кваліфіковані сертифікати відкритих ключів підписувачів та створювачів електронних печаток	Електронна	Постійно	Автоматичне резервне копіювання засобами ІТС надавача та ручне архівне копіювання на окремі носії інформації
Дані про чинність сертифікатів (реєстр сертифікатів, списки відкликаних сертифікатів)	Електронна	Постійно	Автоматичне резервне копіювання засобами ІТС надавача та ручне архівне копіювання на окремі носії інформації
Журнали аудиту подій ІТС надавача	Паперова	10 років на місті створення з подальшою передачею на архівне зберігання	Сховище (сейф)
	Електронна	10 років на місті творення з подальшою передачею на архівне зберігання	Автоматичне резервне копіювання засобами ІТС надавача та ручне архівне копіювання на окремі носії інформації
Укладені договори надання послуг про	Паперова	≥ 3 років після закінчення строку дії сертифіката	Архівне приміщення надавача або відокремленого пункту реєстрації надавача або представництва

	Електронна	≥ 3 років після закінчення строку дії сертифіката	Автоматичне резервне копіювання засобами ІТС надавача та ручне архівне копіювання на окремі носії інформації
Документи та копії документів, що використовуються під час реєстрації заявників	Паперова	≥ 3 років після закінчення строку дії сертифіката	Архівне приміщення надавача або відокремленого пункту реєстрації надавача або представництва
	Електронна	≥ 3 років після закінчення строку дії сертифіката	Автоматичне резервне копіювання засобами ІТС надавача та ручне архівне копіювання на окремі носії інформації
Заяви на формування кваліфікованих сертифікатів відкритих ключів	Паперова	≥ 3 років після закінчення строку дії сертифіката	Архівне приміщення надавача або відокремленого пункту реєстрації надавача або представництва
	Електронна	≥ 3 років після закінчення строку дії сертифіката	Автоматичне резервне копіювання засобами ІТС надавача та ручне архівне копіювання на окремі носії інформації
Заяви на блокування кваліфікованих сертифікатів відкритих ключів	Паперова	≥ 3 років після закінчення строку дії сертифіката	Архівне приміщення надавача або відокремленого пункту реєстрації надавача або представництва
	Електронна	≥ 3 років після закінчення строку дії сертифіката	Автоматичне резервне копіювання засобами ІТС надавача та ручне архівне копіювання на окремі носії інформації
Заяви на скасування кваліфікованих сертифікатів відкритих ключів	Паперова	≥ 3 років після закінчення строку дії сертифіката	Архівне приміщення надавача або відокремленого пункту реєстрації надавача або представництва
Заяви на поновлення кваліфікованих сертифікатів відкритих ключів	Паперова	≥ 3 років після закінчення строку дії сертифіката	Архівне приміщення надавача або відокремленого пункту реєстрації надавача або представництва

Документи у паперовому та електронному вигляді, мають зберігатися у порядку, встановленому законодавством про архіви та архівні справи.

Надавачем забезпечується формування та зберігання у паперовому вигляді актів блокування кваліфікованих сертифікатів відкритих ключів, що відбулись за усною заявою, у порядку, встановленому законодавством про архіви та архівні справи, або фіксація фактів блокування кваліфікованих сертифікатів відкритих ключів, що відбулись за усною заявою засобами ІТС.

Для зберігання носіїв з архівними копіями електронних документів виділяється окреме сховище (сейф чи відсік сейфу) з двома екземплярами ключів і пристроями для опечатування. Один екземпляр ключа від сховища знаходиться у адміністратора безпеки та аудиту, а другий – в опечатаному вигляді зберігається у сховищі (сейфі) керівника профільного підрозділу надавача.

Засоби, що входять до складу центрального серверу ІТС надавача, забезпечують автоматичне резервне копіювання даних. Автоматичне створення резервної копії має виконуватися не рідше одного разу на добу, під час найменшого завантаження центрального серверу.

Додатково може виконуватися резервне копіювання кваліфікованих сертифікатів відкритих ключів на оптичні носії, або інші з'ємні носії інформації у ручному режимі. Після створення нової резервної копії, попередня резервна копія стає архівною.

Відновлення кваліфікованих сертифікатів відкритих ключів з резервної копії здійснюються засобами центрального сервера комплексу шляхом зчитування кваліфікованих сертифікатів відкритих ключів з останньої (актуальної) резервної копії та запису їх у базу даних сервера.

З'ємні носії зберігаються у конвертах чи упаковках, що опечатується печаткою адміністратора безпеки та аудиту. При цьому на упаковці вказується обліковий номер копії. Факти створення та використання копій фіксуються у окремому журналі.

Архівні копії журналів аудиту подій мають зберігатися в приміщенні надавача не менше 10 років на місті створення з подальшою передачею на архівне зберігання. Контроль за здійсненням автоматичного резервного копіювання та виконання резервного копіювання в ручному режимі покладається на системного адміністратора. Адміністратор безпеки та аудиту періодично контролює процес створення та зберігання резервних копій.

Архівне приміщення обладнується технічними засобами, які виключають проникнення сторонніх осіб та неконтрольований доступ до інформації, що підлягає архівуванню.

Знищення архівних документів має здійснюватися комісією, до складу якої входять керівник профільного підрозділу надавача та адміністратор безпеки та аудиту (а також, за необхідності, адміністратор сертифікації). Після завершення процедури знищення архівних документів повинен складатися відповідний акт, який затверджує керівник надавача.

4.1.13 Процес, порядок та умови генерації пар ключів надавача та користувачів

Відповідно до Наказу Міністерства цифрової трансформації України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.09.2020 № 140/614, Зареєстровано в Міністерстві юстиції України 22 жовтня 2020 р. за № 1039/35322 в ІТС надавача використовуються особисті та відповідні їм відкриті ключі за такими призначеннями (сферою використання) та з такими параметрами:

1) в межах країни з метою забезпечення електронного документообігу та електронної автентифікації осіб відповідно до:

ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння» з функцією гешування за

ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования». Ці національні стандарти застосовуються для створення кваліфікованого електронного підпису до 01 січня 2022 року та для створення кваліфікованого електронного підпису з метою надання інформації щодо статусу сертифікатів відкритих ключів до завершення терміну їх дії та для перевірки кваліфікованого електронного підпису;

ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння» з функцією гешування за ДСТУ 7564-2014 «Інформаційні технології. Криптографічний захист інформації. Функція ґешування». Ці національні стандарти застосовуються для створення кваліфікованого електронного підпису з 01 січня 2021 року та для перевірки кваліфікованого електронного підпису;

ДСТУ ISO/IEC 14888-3:2019 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі дискретного логарифмування» із застосуванням алгоритму ECDSA зі ступенем розширення основного поля еліптичної кривої не менше ніж 256 з функціями гешування sha256 або sha512 відповідно до FIPS PUB 180-4 «Secure Hash Standard»;

2) для транскордонного співробітництва з будь-якою метою відповідно до вимог:

ДСТУ ETSI EN 119 312:2015 «Електронні підписи й інфраструктури (ESI). Криптографічні комплекти» та в межах країни з іншою метою, ніж зазначена у підпункті 1 цього пункту та цьому підпункті, шляхом застосовування алгоритмів електронного підпису;

RSA відповідно до RFC 3447 «Public-Key Cryptography Standards (PKCS) № 1: RSA Cryptography Specifications Version 2.1» з довжиною ключа не менше ніж 4096 бітів з функціями гешування sha256 відповідно до FIPS PUB 180-4;

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

- для особистих ключів надавача для накладення електронного підпису на кваліфіковані сертифікати відкритих ключів підписувачів та СВС - не більше 5 років;
- для особистих ключів надавача, що використовуються для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу - не більше 5 років;
- для особистих ключів надавача, що використовуються для накладення електронного підпису на даних про статус кваліфікованих сертифікатів відкритих ключів підписувачів, що визначається в режимі реального часу - не більше 2 років;
- для особистих ключів серверів обробки запитів, що використовуються для криптографічного захисту повідомлень - не більше 2 років;
- для особистих ключів посадових осіб - не більше 2 років.

Особисті ключі надавача для накладення та перевірки електронного підпису на кваліфікованих сертифікатах відкритих ключів підписувачів та СВС, особисті ключі надавача, що використовуються для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу та ключі надавача для накладення та перевірки електронного підпису на даних про статус кваліфікованих сертифікатів відкритих ключів підписувачів, що визначається в режимі реального часу, генеруються, зберігаються та застосовуються виключно у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними пристроями і входять до складу ІТС надавача.

4.1.13.1 Генерація особистих ключів Надавача

Генерація ключів КНЕДП здійснюється у спеціальному приміщенні/шафі/засобі, що унеможливлює витік відомостей про зміст особистого ключа за рахунок побічних електромагнітних випромінювань та наведень.

Перед генерацією ключів КНЕДП усі відповідні засоби ПТК КНЕДП повинні бути встановлені та пройти тестування в установленому порядку.

Генерація ключів КНЕДП, введення даних, необхідних для створення запиту на формування сертифіката відкритого ключа КНЕДП, здійснюється адміністратором сертифікації у присутності та під контролем адміністратора безпеки та аудиту.

Відразу після генерації ключів КНЕДП автоматично створюється (у електронному вигляді) запит на формування сертифіката відкритого ключа КНЕДП, що містить дані (в тому числі, значення відкритого ключа КНЕДП), підписані особистим ключем КНЕДП, необхідні для формування центральним засвідчувальним органом (далі – ЦЗО) сертифіката КНЕДП. Далі цей запит використовується при підготовці документів для сертифікації відкритого ключа КНЕДП в ЦЗО.

Генерація, зберігання, використання ключів КНЕДП здійснюється виключно у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу.

Резервні копії ключів КНЕДП зберігаються у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу.

Після формування сертифікату відкритого ключа КНЕДП він публікується на електронному інформаційному ресурсі КНЕДП.

Після закінчення строку дії сертифіката відкритого ключа КНЕДП особистий ключ КНЕДП та всі його резервні копії знищуються способом, що унеможливлюють їх відновлення.

Адміністратор сертифікації під контролем адміністратора безпеки та аудиту вводить значення коду доступу до особистого ключа таким чином, щоб ніхто не мав можливості з ним ознайомитися.

Код доступу до особистого ключа КНЕДП, повинен бути відомий лише адміністратору сертифікації.

Адміністратор сертифікації записує (таким чином, щоб не допустити ознайомлення з ним інших осіб) на аркуші паперу значення коду доступу до особистого ключа КНЕДП, вміщує цей аркуш в непрозорий конверт, надписує його, опечатує конверт разом з адміністратором безпеки та аудиту і передає на зберігання керівнику (начальнику) КНЕДП.

Не менше ніж за два календарних роки до закінчення строку дії поточного сертифікату відкритого ключа КНЕДП переходить на застосування нового особистого ключа КНЕДП завчасно згенерованого та сертифікованого в ЦЗО.

4.1.13.2 Генерація ключів користувачів

Особистий ключ підписувача або створювача електронної печатки може бути згенерований за допомогою засобів кваліфікованого електронного підпису з використанням:

- стаціонарного робочого місця заявника або на власному портативному обчислювальному пристрої;

- робочої станції генерації ключів в офісі надавача або його відокремлених пунктів реєстрації.

Якщо пара ключів була згенерована заявником поза приміщенням надавача, ідентифікація такого заявника, перевірка достатності обсягу його цивільної правоздатності і дієздатності, формування та видача йому кваліфікованого сертифіката відкритого ключа здійснюється надавачем після перевірки факту володіння заявником особистим ключем, який відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката відкритого ключа, відповідно до пункту 4.1.5 цього Регламенту.

У разі генерації ключових даних підписувачем у «хмарному» сховищі надавача, яке являє собою засіб КЕП, що реалізує зберігання множини особистих ключів КЕП (наприклад,у мережному криптомодулі), така генерація ініціюється підписувачем самостійно після ідентифікації у «хмарному» сховищі на основі атрибутів захисту від доступу сторонніх осіб до використання особистого ключа (пароль, PIN-код, біометричні дані володільця особистого ключа тощо).

Генерацію та/або управління парою ключів від імені підписувача або створювача електронної печатки може здійснювати виключно надавач. Під час управління парою ключів підписувача або створювача електронної печатки надавач може здійснювати резервне копіювання особистого ключа підписувача або створювача електронної печатки з метою його зберігання за умови дотримання таких вимог:

- рівень безпеки резервної копії особистого ключа повинен відповідати рівню безпеки оригінального особистого ключа;
- кількість резервних копій не повинна перевищувати мінімального значення, необхідного для забезпечення безперервності послуги.

Для генерації особистих ключів використовуються засоби кваліфікованого електронного підпису чи печатки, які перебувають у власності користувачів або надаються надавачем.

Надання надавачем засобів кваліфікованого електронного підпису чи печатки здійснюється у порядку, наведеному у розділі 5.1 цього Регламенту. Згенерований особистий ключ підписувача чи створювача електронної печатки захищається за допомогою атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа (пароль, PIN-код, біометричні дані володільця особистого ключа тощо).

Під час надання кваліфікованої електронної довірчої послуги із створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток надавачем забезпечується:

- використання підписувачем або створювачем електронної печатки виключно засобу кваліфікованого електронного підпису чи печатки та кваліфікованого сертифіката електронного підпису чи печатки;
- захист обміну інформацією між підписувачем або створювачем електронної печатки та надавачем засобами телекомунікаційних мереж загального користування;
- 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;
- унікальність пари ключів підписувача або створювача електронної печатки;
- зберігання особистого ключа підписувача або створювача електронної печатки;

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

4.1.14 Процедури отримання користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги її надавачем

Отримання користувачем особистого ключа у володіння в результаті надання кваліфікованої електронної довірчої послуги її надавачем здійснюється за таких умов:

- отримання та використання особистого ключа на правах повного володіння засобом кваліфікованого електронного підпису, у тому числі, носієм особистого ключа;
- отримання та використання особистого ключа на правах повного володіння або доступу на договірних засадах до частини ресурсу засобу кваліфікованого електронного підпису, який реалізує зберігання множини особистих ключів кваліфікованого електронного підпису чи печатки (наприклад, мережний криптомодуль).

Фактичне отримання користувачем особистого ключа відбувається у момент генерації особистого ключа особисто або у момент зміни атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа (пароль, PIN-код, біометричні дані володільця особистого ключа тощо) у випадку, коли ключові пари були попередньо створено надавачем. Не допускається формування надавачем кваліфікованих сертифікатів відкритих ключів до моменту фактичного отримання особистого ключа користувачем.

4.1.15 Механізм надання відкритого ключа користувача надавачу для формування кваліфікованого сертифіката відкритого ключа

Відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа у складі запиту на формування кваліфікованого сертифіката відкритого ключа, який являє собою запит формату PKCS#10, що містить відкритий ключ заявника і додаткову інформацію для формування сертифіката.

Запит формату PKCS#10 формується під час генерації особистого та відкритого ключів засобами кваліфікованого електронного підпису чи печатки. Формування запиту передбачає створення удосконаленого електронного підпису за допомогою особистого ключа з однієї пари з відкритим ключем.

Процес подання запиту на формування кваліфікованого сертифіката відкритого ключа описаний у положеннях сертифікаційних практик цього Регламенту.

4.1.16 Порядок захисту та доступу до особистого ключа надавача

Особисті ключі Надавача розміщуються у засобі КЕП, що є апаратно-програмним або апаратним пристроєм, за допомогою якого здійснювалася генерація пари ключів.

Поточний особистий ключ Надавача зберігається і застосовується виключно в апаратних та апаратно-програмних засобах КЗІ, що входять до складу ПТК Надавача.

Попередні особисті ключі Надавача зберігаються і застосовуються в апаратних та апаратно-програмних засобах КЗІ, що входять до складу ПТК Надавача.

Технологія зберігання особистих ключів Надавача унеможливлює доступ до них ззовні.

Особисті ключі Надавача зберігаються у засобі КЕП, що є апаратно-програмним та апаратним пристроєм.

Апаратні або апаратно-програмні засоби КЗІ із особистими ключами Надавача чи серверів Надавача застосовуються лише у екранованій серверній шафі у спеціально призначеному для цього приміщенні Надавача (серверному приміщенні).

НКІ що містить особистий ключ Надавача, особисті ключі серверів Надавача або їх резервні копії, зберігаються у сейфах (сховищах) у спеціальному приміщенні Надавача. Кожен НКІ зберігається у конверті чи коробці.

Всі НКІ мають бути промарковані та поставлені на облік до початку їх використання, про що робиться відповідний запис до журналу обліку НКІ.

Для забезпечення ідентифікації НКІ можуть використовуватися наявні ідентифікаційні дані у маркуванні – заводські, серійні або інвентарні номери. Інвентарні номери НКІ повинні бути зазначені на наліпках, які наклеюються на корпус носія або прикріплюються у вигляді ярликів.

НКІ однозначно ідентифікується за його типом та ідентифікаційними даними. Всі дії (операції) з НКІ повинні реєструватися у журналі обліку. Всі операції з резервними НКІ повинні реєструватися у журналі обліку так само, як і зі звичайними носіями.

Всі операції з ключовими даними повинні реєструватися у журналі обліку ключових даних.

Облікова картка ключового документа заповнюється адміністратором безпеки та аудиту підписується керівником профільного підрозділу надавача. До облікової картки вноситься інформація про НКІ, ключові дані, що зберігаються на НКІ, включаючи пароль доступу до них, а також, за наявності, пароль доступу до НКІ чи інші ідентифікаційні дані, які необхідні для автентифікації у НКІ (наприклад, інформація про електронні ключі автентифікації для криптомодулів тощо).

НКІ з резервними копіями особистого ключа надавача та особистих ключів серверів ІТС надавача (OCSP, TSP, CMP) зберігаються у спеціальному приміщенні в запечатаних конвертах чи коробках у безпечному сховищі надавача, які опечатуються печаткою керівника профільного підрозділу надавача чи адміністратора безпеки та аудиту.

4.1.17 Заходи безпеки під час генерації ключових даних

Генерація ключових даних (особистих ключів та відкритих ключів) здійснюється згідно з експлуатаційною документацією на відповідні засоби КЕП , на яких здійснюється генерація.

Генерація особистих ключів надавача та особистих ключів серверів ІТС надавача (OCSP, TSP, CMP) здійснюються у спеціальному приміщенні надавача.

Генерація особистих ключів посадових осіб надавача здійснюється на робочих станціях у службових приміщеннях надавача.

Під час генерації особистих ключів надавача та особистих ключів серверів ІТС надавача (OCSP, TSP, CMP) двері до спеціального приміщення повинні бути зачиненими, а всі дії проводитись або у середині приміщення за допомогою термінала або за допомогою віддаленого термінала на робочій станції адміністратора безпеки та аудиту.

Особисті ключі, які зберігаються на НКІ, повинні захищатися на паролях згідно вимог стандартів, що визначають вимоги до засобів кваліфікованого електронного підпису чи печатки, а

саме профілів захисту для пристроїв створення безпечного підпису.

У випадку, якщо для зберігання та використання особистих ключів використовуються мережні криптомодулі, має забезпечуватися взаємна автентифікації криптомодулів та програмних комплексів (складових частин комплексу ІТС надавача). Алгоритм (протокол) взаємної автентифікації повинен реалізовуватися відповідними бібліотеками підтримки (програмними компонентами), які є складовою частиною криптомодулів, згідно стандартів 28-34 наведених у переліку стандартів, який є додатком до Вимог у сфері електронних довірчих послуг, затверджених Постановою Кабінету Міністрів України від 07.11.2018 № 992.

4.1.18 Порядок знищення особистих ключів надавача, серверів ІТС надавача та адміністраторів

Знищення особистих ключів здійснюється згідно з експлуатаційною документацією на відповідні засоби кваліфікованого електронного підпису чи печатки, НКІ чи мережні криптомодулі, у яких вони зберігалися та використовувалися. Процедури знищення особистих ключів повинні забезпечувати неможливість відновлення ключів після знищення.

Факти знищення особистих ключів надавача, серверів ІТС надавача (OCSP, TSP, CMP) та адміністраторів, а також їх резервних копій заносяться до журналу обліку ключових даних. За фактом знищення особистих ключів складаються акти.

4.1.19 Порядок та умови резервного копіювання особистого ключа надавача, серверів ІТС надавача, посадових осіб, збереження, доступу та використання резервних копій

У разі здійснення резервного копіювання особисті ключі Надавача переносяться на зовнішній засіб КЕП, який є апаратно-програмним або апаратним пристроєм у захищеному вигляді, що забезпечує їх цілісність та конфіденційність.

Резервне копіювання та відновлення особистих ключів Надавача здійснюються адміністратором сертифікації під контролем адміністратора безпеки та аудиту.

Після генерації особистого ключа створюється2 резервні копії ключа з криптомодуля. Кожна резервна копія ключа записується на окремий НКІ. НКІ зберігаються в безпечному сховищі сейфі у спеціальному приміщенні Надавача.

Порядок резервного копіювання особистих ключів надавача, серверів ІТС надавача (OCSP, TSP, CMP) та адміністраторів визначено у порядку їх генерації.

Факти резервного копіювання особистих ключів надавача та серверів ІТС надавача (OCSP, TSP, CMP) заносяться до журналу обліку ключових даних.

Факти відновлення особистих ключів надавача та серверів ІТС надавача (OCSP, TSP, CMP) з резервних копій або застосування (переходу до використання) резервних НКІ (мережних криптомодулів) з особистими ключами заносяться до журналу обліку ключових даних. За фактом відновлення особистих ключів чи застосування резервних копій НКІ чи мережних криптомодулів складаються акти.

Резервна копія особистого ключа надавача може бути застосована з дозволу керівника профільного підрозділу надавача у випадку виходу з ладу мережного криптомодуля, в якому зберігався та використовувався особистий ключ для відновлення ключа у відремонтованому або заміненому мережному криптомодулі.

Резервні копії особистих ключів серверів ІТС надавача (OCSP, TSP, CMP) можуть бути застосовані у випадку виходу з ладу НКІ з особистими ключами серверів чи мережних криптомодулів, в яких вони зберігалися та використовувалися для заміни основного НКІ чи відновленні ключів у відремонтованому або заміненому мережному криптомодулі.

Умови забезпечення захисту резервних копій особистих ключів Надавача під час їх зберігання є не гіршими, ніж умови забезпечення захисту особистих ключів, що використовуються. Факти генерації та резервного копіювання особистого ключа Надавача заносяться в журнал генерації, резервного копіювання, відновлення та знищення ключових даних.

4.2 Положення сертифікаційних практик

4.2.1 Процес подання запиту на формування кваліфікованого сертифіката відкритого ключа

До переліку суб'єктів, уповноважених подавати запит на формування кваліфікованого сертифіката відкритого ключа належать заявники.

Запит на формування кваліфікованого сертифіката відкритого ключа приймається в обробку після приймання та реєстрації заяви на формування кваліфікованого сертифіката, встановлення (ідентифікації) особи заявника за її особистої присутності на основі паспорта заявника або інших документів, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи та підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа відповідно до вимог цього Регламенту.

Обробка запиту на формування кваліфікованого сертифіката відкритого ключа здійснюється програмними засобами ІТС надавача за участю адміністратора сертифікації або автоматично.

При отриманні запиту на сертифікацію у відповідному форматі від заявника адміністратор сертифікації перевіряє формат наданого відкритого ключа технічними засобами Надавача, і у разі його невідповідності – відмовляє у формуванні Сертифіката. При цьому надані раніше документи повертаються заявнику з позначкою адміністратора реєстрації.

Під час обробки запиту на формування Сертифіката Підписувача здійснюється перевірка належності особистого ключа Підписувача відкритому ключу, який міститься у запиті. Перевірка здійснюється з використанням технічних засобів Надавача, автоматично, шляхом перевірки удосконаленого електронного підпису, накладеного на запит на формування Сертифіката, з використанням відкритого ключа, що міститься у запиті. Тобто запит на формування Сертифіката є самопідписаним. Формування Сертифіката Підписувача можливе за умов успішної перевірки запиту.

Строк оброблення запиту на формування кваліфікованого сертифіката відкритого ключа, поданого разом із заявою на реєстрацію, становить не більше однієї години.

Процедура повторного формування сертифіката відкритого ключа користувача після закінчення строку обслуговування його сертифікату ключа ідентична процедурі первинного формування сертифіката відкритого ключа.

4.2.2 Порядок надання сформованого кваліфікованого сертифіката відкритого ключа користувачу

Надання сформованого кваліфікованого сертифіката відкритого ключа заявнику здійснюється в один із способів:

- шляхом запису файлу із сформованим кваліфікованим сертифікатом відкритого ключа на носій інформації, наданий заявником;
- шляхом публікації сформованого кваліфікованого сертифіката відкритого ключа на офіційному веб-сайті надавача.

Заявник повинен перевірити свої ідентифікаційні дані, внесені надавачем до кваліфікованого сертифіката відкритого ключа. Надавач повинен надавати відповідні консультації щодо проведення такої перевірки. Заявник повинен використовувати особистий ключ для створення кваліфікованого електронного підпису тільки після проведення перевірки. Використання підписувачем особистого ключа є фактом визнання ним кваліфікованого сертифіката відповідного відкритого ключа.

У разі виявлення заявником невідповідності ідентифікаційних даних, внесених надавачем до кваліфікованого сертифіката відкритого ключа, його власник звертається до надавача для скасування кваліфікованого сертифіката відкритого ключа та формування нового сертифіката у порядку, встановленому цим Регламентом.

У разі невідповідності ідентифікаційних даних, внесених надавачем до кваліфікованого сертифіката відкритого ключа та виявлених надавачем до моменту надання сформованого сертифіката заявнику, посадовою особою надавача здійснюється переформування сертифіката із використанням попередньо засвідченого відкритого ключа та з дотриманням вимог щодо недопущення перевищення часу чинності особистого ключа та відповідного йому відкритого ключа більше двох років. Посадова особа, що здійснила переформування сертифіката, складає акт, в якому зазначається дата та час скасування сертифіката, ідентифікаційні дані заявника, що містяться в сертифікаті та невідповідні ідентифікаційні дані заявника, що зазначені у заяві про формування кваліфікованого сертифіката відкритого ключа. Акт підписується посадовою особою надавача, що здійснила переформування сертифіката, та долучається до документів (посвідчених в установленому порядку копій документів), що використовувалися під час встановлення особи та реєстрації заявника.

4.2.3 Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа користувача на офіційному веб-сайті надавача

Кваліфіковані сертифікати відкритих ключів підписувачів та створювачів електронних печаток, які надали згоду на їх публікацію, публікуються одразу після формування сертифікатів та виконання заявниками умов договору про надання кваліфікованих електронних довірчих послуг.

Згода на публікацію кваліфікованих сертифікатів відкритих ключів надається заявниками під час подання заяв на формування сертифікатів.

4.2.4 Умови використання кваліфікованого сертифіката відкритого ключа користувача та його особистого ключа

Кваліфіковані сертифікати відкритого ключа підписувачів та створювачів електронної печатки використовуються у сферах та із обмеженнями, зазначеними у пунктах 4.1.1 та 4.1.2 цього Регламенту.

Користувачі електронних довірчих послуг зобов'язані дотримуватись умов використання особистих ключів та кваліфікованих сертифікатів відкритих ключів в межах зобов'язань, передбачених у статті 12 Закону України «Про електронні довірчі послуги», а саме:

- забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;
- невідкладно повідомляти надавача про підозру або факт компрометації особистого ключа;
- надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;
- своєчасно здійснювати оплату за електронні довірчі послуги, якщо така оплата передбачена договором між надавачем та користувачем електронних довірчих послуг;
- своєчасно надавати надавачу інформацію про зміну ідентифікаційних даних, які містить кваліфікований сертифікат відкритого ключа;
- не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування кваліфікованого сертифіката відкритого ключа.

Наслідками неправильного використання кваліфікованого сертифіката відкритого ключа та особистого ключа можуть стати недостовірна автентифікація підписувача або створювача електронної печатки в інформаційних системах, заволодіння зловмисниками правами доступу користувача до інформації, підробка електронних документів, матеріальні та репутаційні втрати користувача.

Умови використання кваліфікованого сертифіката відкритого ключа користувача та його особистого ключа, а також відомості про наслідки їх неправильного використання зазначаються у договорі про надання кваліфікованої електронної довірчої послуги.

Заявник (юридична особа) несе відповідальність за організацію, а користувач (посадова особа заявника) або користувач (фізична особа) за безпосереднє надійне збереження особистого ключа та носія ключової інформації, на якому він знаходиться, а також значення коду доступу до цього носія.

Користувач несе відповідальність за розповсюдження власного сертифікату відкритого ключа (якщо користувач не дав згоду на його публікацію в КНЕДП). В цьому випадку, користувач повинен надавати сертифікат всім особам, з якими він вступає у правові відносини у сфері електронних довірчих послуг.

Користувачі несуть відповідальність за вільне (безконтрольне) розповсюдження сертифікатів відкритих ключів інших осіб – суб'єктів правових відносин у сфері електронних довірчих послуг. Користувачі повинні усвідомлювати, що сертифікат відкритого ключа містить персональні дані цих осіб та його розповсюдження без згоди власника призведе до неконтрольованого поширення зазначених відомостей, що може нанести цій особі моральні або матеріальні збитки.

Підписувач зобов'язаний використовувати засоби КЕП для генерації особистих та відкритих ключів КЕП, накладання та перевірки КЕП.

Підписувач зобов'язаний негайно припинити використання особистого ключа в разі його компрометації.

Підписувач зобов'язаний припинити використання особистого ключа з моменту звернення до Надавача щодо блокування або скасування відповідного Сертифіката.

Підписувач зобов'язаний негайно інформувати Надавача про виявлену неточність або зміну даних, зазначених у Сертифікаті.

4.2.5 Процедура подачі запиту на формування кваліфікованого сертифіката відкритого ключа для користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований надавачем

Запит на формування нового кваліфікованого сертифіката відкритого ключа для користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, попередньо сформований надавачем, подається разом із заявою про формування нового кваліфікованого сертифіката відкритого ключа.

Програмні засоби ІТС надавача із інтегрованими засобами кваліфікованого електронного підпису чи печатки, розміщені на офіційному веб-сайті надавача, забезпечують:

- перевірку чинності попереднього кваліфікованого сертифіката відкритого ключа користувача;
- автоматичне формування заяви про формування нового кваліфікованого сертифіката відкритого ключа із використанням ідентифікаційних даних, внесених до попереднього сертифіката;
- створення кваліфікованого електронного підпису чи печатки до цієї заяви із використанням попереднього особистого ключа;
- створення запиту на формування кваліфікованого сертифіката відкритого ключа у форматі PKCS#10 на згенеровану нову ключову пару;
- передачу запиту на формування нового кваліфікованого сертифіката відкритого ключа разом із заявою про формування нового кваліфікованого сертифіката відкритого ключа на обробку до ІТС надавача.

Створення заяви про формування нового кваліфікованого сертифіката відкритого ключа, запиту на формування нового кваліфікованого сертифіката відкритого ключа та їх передача на обробку до ІТС надавача здійснюється із забезпеченням цілісності та конфіденційності інформації за допомогою засобів кваліфікованого електронного підпису чи печатки, та засобів криптографічного захисту, які мають позитивний експертний висновок за результатами їх державної експертизи у сфері КЗІ.

4.2.6 Обставини скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа

До переліку суб'єктів, уповноважених подавати запит на скасування (блокування та поновлення) кваліфікованого сертифіката відкритого ключа формування кваліфікованого сертифіката відкритого ключа належать фізичні та юридичні особи, які подають до надавача заяви або надають інформацію, що підтверджує підстави для зміни статусу сертифіката, передбачені статтею 25 Закону України "Про електронні довірчі послуги".

Перелік підстав для зміни статусу сертифіката із зазначенням суб'єктів подання запитів на зміну статусу та форм підтвердження підстав наведено у таблиці 4.5.

Таблиця 4.5

Підстави для зміни статусу сертифіката	Скасування	Блокування	Поновлення	Підтвердження підстав
подання користувачем електронних довірчих послуг заяви	+	+	+	Заява користувача
смерть фізичної особи - підписувача	+			Документальне підтвердження
припинення діяльності створювача електронної печатки	+			Документальне або технічне (отримання інформації в електронному вигляді з ЄДР) підтвердження
зміни ідентифікаційних даних користувача електронних довірчих послуг	+			Документальне або технічне (отримання інформації в електронному вигляді з ЄДР) підтвердження
факт державної реєстрації припинення підприємницької діяльності фізичної особи - підприємця чи припинення діяльності в установленому законодавством порядку юридичної особи	+			Документальне або технічне (отримання інформації в електронному вигляді з ЄДР) підтвердження
надання користувачем електронних довірчих послуг недостовірних ідентифікаційних даних	+			Документальне підтвердження
факт компрометації особистого ключа користувача електронних довірчих послуг, виявлений самостійно користувачем або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманнямвимог законодавства у сфері електронних довірчих послуг	+			Документальне підтвердження

повідомлення користувачем електронних довірчих послуг або контролюючим органом про підозру в компрометації особистого ключа користувача електронних довірчих послуг		+		Заява користувача або документальне підтвердження
повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа користувачем електронних довірчих послуг або контролюючим органом, який раніше повідомив про цю підозру			+	Заява користувача або документальне підтвердження
набрання законної сили рішенням суду про блокування, поновлення або скасування кваліфікованого сертифікату	+	+	+	Документальне підтвердження
порушення користувачем електронних довірчих послуг істотних умов договору про надання кваліфікованих електронних довірчих послуг		+		Документальне підтвердження

До подій, пов'язаних з компрометацією ключів користувачів, відносяться наступні:

Будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа, зокрема:

- втрата носіїв, на які записані особисті ключі;
- втрата носіїв, на які записані особисті ключі, з наступним виявленням;
- звільнення співробітників, що мали особисті ключі;
- порушення правил зберігання особистих ключів;
- виникнення підозр на несанкціоноване застосування особистого ключа;
- втрату контролю щодо особистого ключа через компрометацію коду доступу до носія особистого ключа;
- випадки, коли не можна вірогідно встановити, що відбулося з носіями, що містять ключову інформацію (у тому числі, випадки, коли носій вийшов з ладу й доказово не спростована можливість того, що даний факт відбувся в результаті несанкціонованих дій зловмисника).

У випадку компрометації ключа користувач зобов’язаний терміново сповістити про цей факт КНЕДП.

До зміни ідентифікаційних даних користувача належать:

- звільнення з роботи власника сертифіката відкритого ключа (для сертифікатів ключів юридичних осіб/посадових осіб);
- зміна прізвища;
- зміна місця прописки/реєстрації в частині, якщо воно вказане в реквізитах власника сертифіката відкритого ключа;
- виявлення помилок у реквізитах тощо.

Зміна зовнішніх обставин,які навіть при збереженні реквізитів власника сертифіката відкритого ключа змінюють його статус, що впливає на правомочність КЕП, зокрема, зміна положення про посаду, переведення на іншу посаду, що призводить до того, що зазначені в сертифікаті відкритого ключа повноваження більше йому не належать (в тому числі втрата права підпису звітності, керування банківським рахунком тощо) потребує скасування сертифіката.

За виникнення будь-яких вищезазначених причин та обставин користувач зобов'язаний невідкладно заблокувати сертифікат відкритого ключа та протягом терміну дії блокування виконати операції зі скасування сертифіката відкритого ключа.

Заява про скасування (блокування, поновлення) кваліфікованого сертифіката електронного підпису чи печатки подається надавачеві у спосіб, що забезпечує підтвердження особи користувача.

Перелік та опис механізмів автентифікації користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа наведено у таблиці 4.5 цього Регламенту.

Надавач здійснює цілодобовий прийом та перевірку заяв заявників та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів в тому числі з використанням інформаційних каналів, відомості про які наведено на офіційному сайті надавача.

Кваліфіковані сертифікати відкритих ключів скасовуються, блокуються та поновлюються надавачем не пізніше ніж протягом двох годин від моменту отримання підтвердження підстав для зміни статусу сертифіката та здійснення відповідної перевірки достовірності документальних повідомлень та автентифікації заявників.

Надавач формує списки відкликаних сертифікатів у вигляді повного та часткового списків. Повний список відкликаних сертифікатів формується та публікується 1 раз на тиждень та містить інформацію про всі відкликані сертифікати ключів, які були сформовані надавачем. Частковий список відкликаних сертифікатів формується та публікується кожні 2 години та містить інформацію про всі відкликані кваліфіковані сертифікати, статус яких був змінений в інтервалі між часом формування останнього повного списку відкликаних сертифікатів та часом формування поточного часткового списку відкликаних сертифікатів.

Крім списків відкликаних сертифікатів, розповсюдження інформації про статус кваліфікованих сертифікатів електронного підпису чи печатки користувачів також здійснюється шляхом забезпечення можливості перевірки статусу кваліфікованого сертифіката електронного підпису чи печатки користувача в режимі реального часу через телекомунікаційні мережі загального користування із використанням протоколу OCSP.

Посилання на сервіс перевірки статусу кваліфікованого сертифіката електронного підпису чи печатки користувача в режимі реального часу вносяться до кваліфікованих сертифікатів відкритих ключів підписувачів та створювачів електронної печатки.

4.2.7 Строк закінчення дії кваліфікованого сертифіката відкритого ключа користувача

Строк дії кваліфікованих сертифікатів відкритих ключів користувачів становить не більше двох років.

Дата та час початку та закінчення строку дії кваліфікованого сертифіката відкритого ключа користувача зазначається у сертифікаті із точністю до однієї секунди.

Після закінчення строку дії кваліфікованого сертифіката такий кваліфікований сертифікат відкритого ключа вважається нечинним.

5. ПРОЦЕДУРИ ТА ПРОЦЕСИ, ЯКІ ВИКОНУЮТЬСЯ ПІД ЧАС НАДАННЯ КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, ЩО НЕ ПЕРЕДБАЧАЮТЬ ФОРМУВАННЯ ТА ОБСЛУГОВУВАННЯ КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ

5.1 Надання засобів кваліфікованого електронного підпису чи печатки

Для надання кваліфікованих електронних довірчих послуг надавачем використовуються засоби кваліфікованого електронного підпису чи печатки, які мають позитивний експертний висновок за результатами їх державної експертизи у сфері КЗІ.

Надання надавачем засобів кваліфікованого електронного підпису чи печатки у вигляді апаратно-програмних засобів та їх технічна підтримка і обслуговування здійснюється на договірних засадах.

Надання надавачем засобів кваліфікованого електронного підпису чи печатки у вигляді окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків, може здійснюватись шляхом передачі цих засобів на носіях інформації безпосередньо підписувачу або створювачу електронної печатки або шляхом надання доступу через офіційний веб-сайт надавача.

Засоби кваліфікованого електронного підпису чи печатки у вигляді SIM-карток надаються користувачам надавачем або оператором мобільного зв’язку, який обслуговує такі засоби, та який виконує функції відокремленого пункту реєстрації.

Генерація особистих ключів у складі пар ключів у засобах кваліфікованого електронного підпису у вигляді SIM-карток здійснюється вбудованими механізмами цих апаратнопрограмних засобів. Допомога при генерації ключів у SIM-картці здійснюється адміністратором реєстрації або працівником відокремленого пункту реєстрації, на якого покладено обов’язки з реєстрації користувачів, та який виконує функції адміністратора реєстрації.

5.2 Надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу

Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження кваліфікованої електронної позначки часу надається користувачам в режимі реального часу за

протоколом TSP.

Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу включає:

- формування кваліфікованої електронної позначки часу за запитом користувача;
- передачу кваліфікованої електронної позначки часу користувачеві електронної довірчої послуги.

Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу надається цілодобово.