Прим. № 1

ПОГОДЖЕНО
Голова Державної служби
спеціального зв'язку та захисту
інформації України

Ю.Ф. Шиголь
«26» 11 2020 р.

ЗАТВЕРДЖУЮ
В.о. генерального директора
державного підприємства «ДІЯ»

В.С. Легкий
«13» 07 2020 р.

РЕГЛАМЕНТ РОБОТИ

КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ
«ДІЯ»

На 43 аркушах

Київ 2020 р.

ЗМІСТ

ВСТУП

Перелік скорочень

ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань
ЄДДР	Єдиний державний демографічний реєстр
ІТС	Інформаційно-телекомунікаційна система
КЗІ	Криптографічний захист інформації
ЗНОК	Захищений носій особистих ключів
НКІ	Носій ключової інформації
ОС	Операційна система
ПЗ	Програмне забезпечення
РНОКПП	Реєстраційний номер облікової картки платника податків
УНЗР	Унікальний номер запису в ЄДДР
ЦОД	Центр обробки даних
CMP	Certificate Management Protocol
OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol

Терміни та визначення

В цьому регламенті терміни та визначення застосовуються у значеннях, наведених у Цивільному кодексі України, Законі України від 05 жовтня 2017 року № 2155-VIII "Про електронні довірчі послуги", постанові Кабінету міністрів України від 07 листопада 2018 року № 992 «Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг», інших нормативно-правових актах з питань криптографічного та технічного захисту інформації.

Статус Регламенту

Цей регламент є документом кваліфікованого надавача електронних довірчих послуг «ДІЯ» (далі – надавач), що визначає організаційно-методологічні, технічні та технологічні умови діяльності надавача під час надання кваліфікованих електронних довірчих послуг, включаючи політику сертифіката та положення сертифікаційних практик.

Регламент розроблений відповідно до:

- Закону України від 05 жовтня 2017 року № 2155-VIII “Про електронні довірчі послуги”;
- 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”;
- Вимоги 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;
- інших нормативно-правових актів сфери надання електронних довірчих послуг.

Норми цього регламенту поширюються на:

- працівників головного офісу надавача;
- працівників відокремлених пунктів реєстрації надавача;
- заявників;
- підписувачів;
- створювачів електронної печатки.

Вимоги регламенту є обов’язковими до виконання працівниками головного офісу та відокремлених пунктів реєстрації надавача.

Визнання вимог регламенту заявниками, підписувачами та створювачами електронних печаток обов’язковою умовою та підставою для укладання з ними договору про надання 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».

Будь-яка зацікавлена особа може ознайомитися з положеннями регламенту на офіційному сайті надавача.

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим регламентом, застосовуються правила міжнародного договору.

Внесення змін та доповнень до Регламенту

Внесення змін та доповнень до цього Регламенту здійснюється надавачем відповідно до Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07 листопада 2018 року № 992.

Про внесення змін та доповнень до цього регламенту, надавач повідомляє заявників, підписувачів, створювачів електронних печаток та інших зацікавлених осіб шляхом розміщення зазначених змін та доповнень на офіційному веб-сайті надавача.

Всі зміни та доповнення, внесені надавачем до регламенту, що не пов'язані зі зміною законодавства, набувають чинності через 10 (десять) календарних днів з дня розміщення зазначених змін і доповнень на офіційному веб-сайті надавача.

Всі зміни та доповнення, внесені надавачем до регламенту у зв'язку зі зміною законодавства, набувають чинності одночасно зі вступом в силу відповідних нормативно-правових актів, але не раніше моменту опублікування змін на офіційному веб-сайті надавача.

1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО НАДАВАЧА

Повні найменування юридичної особи надавача: державне підприємство «ДІЯ», State enterprise «DIIA».

Скорочені найменування юридичної особи: ДП «ДІЯ», SE «DIIA».

Повні найменування надавача: Кваліфікований надавач електронних довірчих послуг «ДІЯ», Qualified Trust Services Provider «DIIA».

Скорочені найменування надавача: КНЕДП «ДІЯ», QTSP «DIIA».

Телефон: +38 067 107-20-41.

Код ЄДРПОУ: 43395033.

Електронна адреса веб-сайту надавача: ca.informjust.ua

Адреса електронної пошти головного офісу надавача: ca@diia.gov.ua, keys@diia.gov.ua, ca@informjust.ua

Головний офіс надавача представлений окремим підрозділом або позаштатною структурою ДП «ДІЯ», що здійснює надання кваліфікованих електронних довірчих послуг та забезпечує виконання вимог законодавства до надавачів.

Представництвами надавача є відокремлені пункти реєстрації, що представлені окремими підрозділами або позаштатними одиницями ДП «ДІЯ», або юридичні чи фізичні особи, які на підставі договору з ДП «ДІЯ», 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 ДП «ДІЯ» або від імені представництва.

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

Найманими працівниками надавача, посадові обов’язки яких безпосередньо пов’язані з наданням кваліфікованих електронних довірчих послуг у головному офісі надавача, є працівники, на яких покладено функціональні обов’язки:

- керівника профільного підрозділу надавача;
- адміністратора реєстрації;
- адміністратора сертифікації;
- адміністратора безпеки та аудиту;

- системного адміністратора.

Керівник профільного підрозділу надавача в межах виконання своїх обов'язків відповідає за організацію та контроль процесів, направлених на забезпечення функціонування, розвитку надавача та захист інформації в 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;

Керівник профільного підрозділу надавача безпосередньо приймає участь та контролює процес генерації та резервного копіювання ключів надавача з правами та обов’язками адміністратора сертифікації.

Керівник профільного підрозділу надавача представляє надавача у випадках, передбачених Регламентом роботи центрального засвідчувального органу.

Адміністратор реєстрації відповідає за перевірку документів, наданих заявниками, їх заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів.

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.

Додатковими обов’язками адміністратора реєстрації є:

- надання допомоги під час генерації пари ключів підписувача або створювача електронної печатки;
- обробка запитів на формування та зміну статусу сертифікатів ключів підписувачів;
- надання консультацій щодо умов та порядку отримання кваліфікованих електронних довірчих послуг;
- ведення архіву надавача.

Адміністратор сертифікації відповідає за формування кваліфікованих сертифікатів відкритих ключів, ведення електронного реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів, збереження та використання особистих ключів надавача, а також створення їх резервних копій.

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;
- перевірка заяв про формування кваліфікованих сертифікатів відкритих ключів надавача на відповідність вимогам регламенту роботи надавача;
- 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.

Додатковими обов'язками адміністратора сертифікації є ведення журналів обліку адміністратора сертифікації, передбачених документацією комплексної системи захисту інформації ІТС надавача.

Адміністратор безпеки та аудиту відповідає за належне функціонування комплексної системи захисту інформації.

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 адміністраторів;
- участь у знищенні особистих ключів надавача, контроль за правильним і своєчасним знищенням адміністраторами 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 та представництв 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.

Системний адміністратор відповідає за функціонування засобів та обладнання програмно-технічного комплексу (далі - технічні засоби) ІТС надавача.

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 працівники юридичних осіб та фізичні особи - підприємці, які на підставі договору з надавачем здійснюють реєстрацію підписувачів з дотриманням вимог Закону України «Про електронні довірчі послуги» та законодавства у сфері захисту інформації.

На працівників відокремлених пунктів реєстрації надавача покладено функціональні обов'язки:

- віддаленого адміністратора реєстрації та оператора реєстрації;

- відповідального за захист інформації на відокремленому пункті реєстрації.

Віддалений адміністратор реєстрації та оператор реєстрації відповідають за виконання функцій та несуть обов'язки адміністратора реєстрації, визначені у цьому регламенті.

З числа віддалених адміністраторів реєстрації на відокремленому пункті реєстрації призначаються відповідальні за захист інформації.

В межах виконання своїх обов'язків відповідальний за захист інформації на відокремленому пункті реєстрації відповідає за належну експлуатацію комплексу засобів захисту відокремленого пункту реєстрації.

Основними обов'язками відповідального за захист інформації на відокремленому пункті реєстрації є:

- організація експлуатації та технічного обслуговування апаратних та програмних засобів відокремленого пункту реєстрації;
- участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації відокремленого пункту реєстрації;
- контроль за роботою програмного комплексу відокремленого пункту реєстрації;
- контроль за використанням особистих ключів персоналу відокремленого пункту реєстрації;
- участь у створенні та введенні в експлуатацію комплексної системи захисту інформації на представництвах.

Допускається виконання функцій відповідального за захист інформації на відокремленому пункті реєстрації системним адміністратором та адміністратором безпеки та аудиту у частині, що не є в протиріч з їх аналогічними функціями по відношенню до інших складових ІТС надавача.

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, сформованих 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 1:

Таблиця 1

Сфера використання кваліфікованого сертифіката відкритого ключа	“Призначення відкритого ключа” (“keyUsage”)
Автентифікація	digitalSignature + nonRepudiation або keyAgreement
Перевірка кваліфікованого електронного підпису	digitalSignature + nonRepudiation

Сфера використання кваліфікованого сертифіката відкритого ключа	“Призначення відкритого ключа” (“keyUsage”)
Перевірка кваліфікованої електронної печатки	digitalSignature + nonRepudiation
Узгодження ключів шифрування	keyAgreement

Надавач формує кваліфіковані сертифікати відкритого ключа з розширеннями сертифіката digitalSignature + nonRepudiation або keyAgreement за умов, 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.

У випадках, передбачених вимогами до окремо визначених інформаційно-телекомунікаційних систем, окрім ознаки того, що генерація особистого ключа відбулася з використанням захищеного носія особистого ключа (id-etsi-qcs 4), для ідентифікації типу захищеного носія особистого ключа, під час формування кваліфікованого сертифіката відкритого ключа надавач встановлює додаткове розширення “Уточнене призначення відкритого ключа” “extendedKeyUsage” та умовне позначення типу такого носія із його унікальним заводським номером у додаткових даних підписувача.

4.1.2 Обмеження щодо використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем

Не допускається використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем для певної сфери із відповідним розширенням сертифіката, 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.

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

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 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 чи печатка 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 (один) раз на тиждень та містить інформацію про всі відкликані сертифікати ключів, які були сформовані надавачем.

Частковий список відкликаних сертифікатів формується та публікується кожні 2 (дві) години та 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.

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

Підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа, забезпечується:

- візуальним та технічним контролем запису та передачі надавачеві запиту на формування кваліфікованого сертифіката відкритого ключа особисто заявником під час генерації пари ключів одразу після ідентифікації заявника, за умови його особистої присутності

або

- технічним контролем запису та передачі надавачеві запиту на формування кваліфікованого сертифіката відкритого ключа особисто заявником під час генерації пари ключів одразу після ідентифікації заявника за ідентифікаційними даними, що містяться у раніше сформованому надавачем кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката.

В обох випадках за допомогою засобів кваліфікованого електронного підпису надавача здійснюється перевірка удосконаленого електронного підпису, створеного за допомогою особистого ключа заявника на запиті на формування кваліфікованого сертифіката, за допомогою відкритого ключа, що міститься у цьому запиті.

Підтвердження володіння заявником особистим ключем здійснюється без розкриття особистого ключа.

4.1.6 Умови встановлення 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 фізичної особи 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.

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.

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.

Надання кваліфікованих електронних довірчих послуг надавачем передбачає подання заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів.

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.

Перелік ідентифікаційних даних та механізми їх підтвердження для формування кваліфікованих сертифікатів відкритих ключів електронного підпису чи печатки наведено у Таблицях 2 та 3.

Таблиця 2

Ідентифікаційні дані та механізми їх підтвердження під час встановлення фізичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа

Ідентифікаційні дані	Обов'язковість надання ідентифікаційних даних	Механізми підтвердження ідентифікаційних даних
Прізвище, ім'я, по батькові (за наявності)	Обов'язково	Документальне (паспорт, посвідка на постійне (тимчасове) місце проживання)
РНОКПП	За наявності	Документальне (облікова картка платника податків, паспорт)
Серія (за наявності), номер паспорта	Обов'язково	Документальне (паспорт)
УНЗР	За наявності	Документальне (паспорт)
Номер телефону	Обов'язково	Технічне (відтворення тексту SMS повідомлення, надісланого надавачем)
Адреса електронної пошти	Обов'язково	Технічне (відповідь на електронний лист, надісланий надавачем)
Повноваження або займана посада	На вимогу заявника про їх включення до сертифіката	Документальне (документ, що засвідчує право на здійснення діяльності у визначеній сфері: посвідчення, сертифікат, наказ про призначення, свідоцтво тощо) або технічне (інформація з відповідних державних інформаційних систем (реєстрів, баз даних тощо))

Таблиця 3

Ідентифікаційні дані та механізми їх підтвердження під час встановлення юридичних осіб, уповноважені працівники яких вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа

Ідентифікаційні дані	Обов'язковість надання ідентифікаційних даних	Механізми підтвердження ідентифікаційних даних
Найменування юридичної особи	Обов'язково	Документальне або технічне (отримання інформації в електронному вигляді з ЄДР)
Код ЄДРПОУ	Обов'язково	Документальне або технічне (отримання інформації в електронному вигляді з ЄДР)
Місцезнаходження	Обов'язково	Документальне або технічне (отримання інформації в електронному вигляді з ЄДР)

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 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

Таблиця 4

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	Друга

			підпис адміністратора реєстрації в підсистемі створення облікових записів користувачів	
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.

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.

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 підписувача 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 з питань блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа

Перелік та опис механізмів автентифікації користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа наведено у Таблиці 5

Таблиця 5

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

Цей розділ регламенту не входить до обсягу положень, визначених надавачем для ознайомлення користувачами.

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 щодо комплексної системи захисту інформації або системи управління інформаційною безпекою в межах організації з урахуванням режиму роботи надавача передбачає дисциплінарні стягнення, адміністративну та кримінальну відповідальність, передбачені:

- колективним договором між Адміністрацією державного підприємства «ДІЯ» і трудовим колективом;

- договором на здійснення представництва надавача;

- 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 і попередженнями про відповідальність під особистий підпис.

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 6

Таблиця 6

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/ зберігання у сховищах (сейфах)	Адміністратор безпеки та аудиту
Встановлення прав доступу та інших параметрів безпеки	≤ 1 раз на тиждень	Постійно	Електронна	засобами ОС/ засобами ПЗ ІТС надавача/ зберігання у сховищах (сейфах)	Адміністратор безпеки та аудиту
Генерація, використання та знищення ключових даних	за необхідності	Постійно	Паперова/ електронна	засобами ОС/ засобами ПЗ ІТС надавача/	Адміністратор безпеки та аудиту

Тип події	Частота перегляду	Строк зберігання	Форма ведення	Метод захисту	Доступ на перегляд
				зберігання у сховищах (сейфах)	
Внесення, модифікація та видалення реєстраційних даних підписувачів	≤ 1 раз на добу	Постійно	Електронна	засобами ОС/ засобами ПЗ ІТС надавача/ зберігання у сховищах (сейфах)	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/ зберігання у сховищах (сейфах)	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 у сховищах (сейфах)	Адміністратор безпеки та аудиту
Отримання персоналом доступу до автоматизованої системи надавача та її складових частин (вхід до операційної систему тощо)	≤ 1 раз на тиждень	Постійно	Електронна	засобами ОС/ засобами ПЗ ІТС надавача/ зберігання у сховищах (сейфах)	Адміністратор безпеки та аудиту
Спроби несанкціонованого доступу до автоматизованої	≤ 1 раз на добу	Постійно	Електронна	засобами ОС/ засобами ПЗ ІТС	Адміністратор безпеки та аудиту

Тип події	Частота перегляду	Строк зберігання	Форма ведення	Метод захисту	Доступ на перегляд
системи надавача та її складових частин				надавача/ зберігання у сховищах (сейфах)	
Збої у роботі автоматизованої системи надавача та її складових частин	≤ 1 раз на добу	Постійно	Паперова/ електронна	засобами ОС/ засобами ПЗ ІТС надавача/ зберігання у сховищах (сейфах)	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 7.

Таблиця 7

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

Види документів та даних	Форма зберігання	Строк зберігання	Механізм зберігання
Журнали аудиту подій ІТС надавача	Паперова	≥ 2 років	Сховище (сейф)
	Електронна	≥ 2 років	Автоматичне резервне копіювання засобами ІТС надавача та ручне архівне копіювання на окремі носії інформації
Укладені договори про надання послуг	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	Автоматичне резервне копіювання засобами ІТС надавача та ручне архівне

Види документів та даних	Форма зберігання	Строк зберігання	Механізм зберігання
		строку дії сертифіката	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 2-х років. 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

Цей розділ регламенту не входить до обсягу положень, визначених надавачем для ознайомлення користувачами, окрім положень, що стосується опису процесу, порядку та умови генерації пар ключів користувачів.

4.1.13.14 Генерація ключів користувачів

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;
- створення умов для генерації пари ключів підписувача або створювача електронної печатки;
- 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.

Особистий ключ у складі пари ключів підписувача або створювача електронної печатки може бути згенерований:

- на стаціонарному робочому місці підписувача (створювача електронної печатки) або на власному портативному обчислювальному пристрої;
- на робочій станції генерації ключів в офісах надавача та його відокремлених пунктів реєстрації.

У разі коли пара ключів була згенерована заявником поза приміщенням надавача та/або за відсутності відповідного персоналу, 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.

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, 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 у вигляді апаратно-програмних засобів (ЗНОК, токени, SIM-картки, мережні криптомодулі), які можуть функціонувати під управлінням або з використанням окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків та які перебувають у власності користувачів, або надаються надавачем.

Надання надавачем засобів кваліфікованого електронного підпису чи печатки здійснюється у порядку, наведеному у розділі 5 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).

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) 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 файл 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

4.1.16.14 Порядок обліку та зберігання ключових даних та документів

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.

4.1.16.15 Порядок зберігання носіїв ключової інформації

НКІ повинні зберігатися у сейфах (сховищах) у службових приміщеннях надавача. Кожен НКІ повинен зберігатися у конверті (коробці, тубусі) разом із обліковою карткою – у вигляді ключового документа.

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

4.1.16.16 Заходи безпеки під час генерації ключових даних

Генерація ключових даних (особистих ключів та відкритих ключів) здійснюється згідно з експлуатаційною документацією на відповідні технічні засоби комплексу ІТС надавача, 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 носіях ключової інформації, повинні захищатися на паролях згідно вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису, затверджених спільним наказом Міністерства юстиції України та Адміністрації Держспецзв'язку № 2782/5/689 від 27.12.2013 р.

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. Інтерфейси бібліотек підтримки криптомодулів повинні відповідати вимогам до алгоритмів, форматів і інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису, затверджених спільним наказом Міністерства юстиції України та Адміністрації Держспецзв'язку № 2782/5/689 від 27.12.2013 р.

4.1.16.17 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.

4.1.17 Порядок та умови резервного копіювання особистого ключа надавача, серверів ІТС надавача, адміністраторів, збереження, доступу та використання резервних копій

Порядок резервного копіювання особистих ключів надавача, серверів ІТС надавача (OCSP, TSP, CMP) та адміністраторів визначено у порядку їх генерації (пункти 4.1.13.1 та 4.1.13.2 цього регламенту).

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.

Резервні копії особистих ключів адміністраторів можуть не створюватися. При цьому адміністраторам можуть видаватися резервні НКІ з попередньо згенерованими особистими ключами. Запити на формування кваліфікованих сертифікатів відкритих ключів адміністраторів зберігаються у адміністратора безпеки. У разі компрометації особистого ключа чи виходу з ладу основного НКІ для адміністратора випускається новий кваліфікований сертифікат, адміністратор починає використовувати резервний НКІ.

4.2 Положення сертифікаційних практик

4.2.13 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 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 реєстрації, працівника представництва надавача (відокремленого пункту реєстрації), на якого покладено обов'язки з реєстрації користувачів, та який виконує функції адміністратора реєстрації, або автоматично за умови забезпечення безперервності процесів генерації пар ключів, формування запитів, передачі їх на обробку захищеними каналами зв'язку, які забезпечують конфіденційність та цілісність даних. Автоматична обробка запитів не виключає процесів встановлення (ідентифікації) особи заявника та підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа.

Під час обробки запиту на формування кваліфікованого сертифіката відкритого ключа засобами ІТС надавача здійснюється перевірка унікальності відкритого ключа в реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів та забезпечується унікальність серійного номера кваліфікованого сертифіката електронного підпису чи печатки.

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

4.2.14 Порядок надання сформованого кваліфікованого сертифіката відкритого ключа користувачу

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

- шляхом надсилання файлу із сформованим кваліфікованим сертифікатом відкритого ключа на адресу електронної пошти, вказану у заяві на формування кваліфікованого сертифіката відкритого ключа;
- 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.

4.2.15 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 надаються заявниками під час подання заяв на формування сертифікатів.

4.2.16 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.

4.2.17 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.

4.2.18 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 9.

Таблиця 9

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
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 дотриманням вимог законодавства у сфері електронних довірчих послуг	+			Документальне підтвердження
повідомлення користувачем електронних довірчих послуг або контролюючим органом про підозру в компрометації		+		Заява користувача або документальне підтвердження

Підстави для зміни статусу сертифіката	Скасування	Блокування	Поновлення	Підтвердження підстав
особистого ключа користувача електронних довірчих послуг				
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	+	+	+	Документальне підтвердження
порушення користувачем електронних довірчих послуг істотних умов договору про надання кваліфікованих електронних довірчих послуг		+		Документальне підтвердження

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 5 цього регламенту.

Надавач здійснює цілодобовий прийом та перевірку заяв підписувачів 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 скасовується, 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 (один) раз на тиждень та містить інформацію про всі відкликані сертифікати ключів, які були сформовані надавачем.

Частковий список відкликаних сертифікатів формується та публікується кожні 2 (дві) години та 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.

Розповсюдження інформації про статус кваліфікованих сертифікатів електронного підпису чи печатки користувачів здійснюється шляхом створення 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.

4.2.19 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 перевершення дати та часу закінчення строку дії кваліфікованого сертифіката користувача, 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 представництва надавача (відокремленого пункту реєстрації).

Генерація особистих ключів у складі пар ключів у засобах кваліфікованого електронного підпису у вигляді SIM-карток здійснюється вбудованими механізмами цих апаратно-програмних засобів. Допомога при генерації ключів у SIM-картці здійснюється адміністратором реєстрації або працівником представництва надавача (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 підписувачам та створювачам електронних печаток при створенні кваліфікованого електронного підпису чи печатки.

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

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

Кваліфікована електронна позначка часу має презумпцію точності дати та часу, на які вона вказує, та цілісності електронних даних, з якими ці дата та час пов’язані.