ПОГОДЖЕНО

Голова Державної служби спеціального зв'язку та захисту інформації України

_____ Ю.Ф. Щиголь

“___”_____ 2020 р.

ЗАТВЕРДЖУЮ

Директор ТОВ «Центр сертифікації ключів «Україна»

_____ В.В. Кохно

“___”_____ 2020 р.

РЕГЛАМЕНТ
РОБОТИ КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ ТОВАРИСТВА З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ «УКРАЇНА»

На 32 аркушах

Київ 2020

Зміст

ВСТУП

Перелік умовних позначень та скорочень

У цьому Регламенті умовні позначення та скорочення, наявні в ньому, використовуються у такому значенні:

Умовні позначення та скорочення	Опис
Надавач	Кваліфікований надавач електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна»
БД	База даних
ВПР	Відокремлений пункт реєстрації
Договір	Договір про надання електронних довірчих послуг
ЕП	Електронний підпис
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань
ЄДДР	Єдиний державний демографічний реєстр
ЄДРПОУ	Єдиний державний реєстр підприємств та організацій України
Заявка	Заявка (запит) на формування сертифіката відкритого ключа
ІТС	Інформаційно-телекомунікаційна система
Картка приєднання	Картка приєднання до договору про надання електронних довірчих послуг
КЗІ	Криптографічний захист інформації
КСЗІ	Комплексна система захисту інформації
ОС	Операційна система
ПЗ	Програмне забезпечення
ПТК	Програмно-технічний комплекс
Регламент	Регламент роботи кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна»
РНОКПП	Реєстраційний номер облікової картки платника податків
Сертифікат	Кваліфікований сертифікат відкритого ключа

СКБД	Система керування базою даних
УНЗР	Унікальний номер запису в ЄДДР
ЦЗО	Центральний засвідчувальний орган
OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol

Терміни та визначення

У 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

Регламент роботи кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (далі – надавач) 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”;
- 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;
- інших нормативно-правових актів у сфері надання електронних довірчих послуг.

Норми цього Регламенту поширюються на:

- працівників надавача;
- заявників;
- підписувачів;
- створювачів електронної печатки.

Вимоги Регламенту є обов’язковими до виконання працівниками надавача.

Визнання вимог Регламенту заявниками, підписувачами та створювачами електронних печаток є 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 веб-сайті надавача.

Відповідно до Вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації, затверджених Наказом

Адміністрації Держспецзв'язку від 14 травня 2020 року № 269, надавачем встановлюються вимоги до процедур з управління ризиками, персоналом, операційною безпекою, інцидентами, доказами та архівами, поводження з персональними даними користувачів, процедур встановлення заявника, ВПР та виїзних адміністраторів реєстрації, опису фізичного середовища. Зазначені вимоги визначаються цим Регламентом, а також іншими організаційно-розпорядчими документами надавача.

Порядок внесення змін та доповнень до Регламенту

Внесення змін та доповнень до 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 Регламенту надавач повідомляє заявників, підписувачів, створювачів електронних печаток та інших зацікавлених осіб шляхом розміщення зазначених змін та доповнень на офіційному веб-сайті 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.

1.ЗАГАЛЬНІ ВІДОМОСТІ ПРО НАДАВАЧА

Повні найменування надавача: товариство з обмеженою відповідальністю «Центр сертифікації ключів «Україна», Limited Liability Company «Key Certification Center «Ukraine».

Скорочені найменування надавача: ТОВ «Центр сертифікації ключів «Україна», «Key Certification Center «Ukraine» LLC.

Юридична та фактична адреса надавача: Україна, 04080, м. Київ, вул. Кирилівська, 102.

Телефон: +38 (044) 206-72-31.

Код ЄДРПОУ: 36865753.

Електронна адреса веб-сайту надавача: **uakey.com.ua**

Адреса електронної пошти надавача: **info@uakey.com.ua**

Для надання електронних довірчих послуг на певній території надавач може створювати відокремлені пункти реєстрації та (або) відряджати посадових осіб (адміністраторів реєстрації) до певного регіону.

Відокремленими пунктами реєстрації надавача є філії чи окремі підрозділи надавача, а також юридичні чи фізичні особи, які на підставі договору з ТОВ «Центр сертифікації ключів «Україна» здійснюють реєстрацію підписувачів з дотриманням вимог законодавства у сфері електронних довірчих послуг та захисту інформації.

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, є працівники, на яких покладено функціональні обов’язки:

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

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;
- 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 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;
- 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 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 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.

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 або системи управління інформаційною безпекою;
- 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 - 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 покладено функціональні обов’язки:

- віддаленого адміністратора реєстрації;
- відповідального за захист інформації на відокремленому пункті реєстрації.

Віддалений адміністратор реєстрації відповідає за виконання функцій та несе 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 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, 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 та ФОП, 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 № X», де X – 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.

Надавач має право встановлювати обмеження сфери використання сформованих ним сертифікатів ключів. 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, його ВПР і виїзних адміністраторів реєстрації (реквізити, адреси, контактні телефони, ідентифікаційні дані виїзних адміністраторів тощо);;
- 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.

На веб-сайті додатково може розміщуватись будь-яка інша інформація.

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.

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. Для перевірки чинності документів, що посвідчують особу, за наявності технічної можливості використовується сервіс "Перевірка за базою недійсних документів" (nd.dmsu.gov.ua).

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.

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).

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:

- заповнений та підписаний договір - у двох примірниках або заповнену та підписану заявником картку приєднання до електронного договору - в одному примірнику;
- оригінал виписки чи витягу з ЄДР, або копію одного з цих документів, засвідчену нотаріально або державним реєстратором, або підписом керівника та печаткою юридичної особи (за наявності);
- копії паспортів підписувачів або інших документів, що посвідчують особу відповідно до законодавства України, засвідчені відповідними підписувачами або нотаріально;
- копії довідок про присвоєння ідентифікаційних номерів (карток фізичних осіб – платників податку) підписувачів, засвідчені відповідними підписувачами або нотаріально (у випадку, якщо наданий паспорт підписувача не містить значення ІН);
- копії документів про призначення на посаду підписувачів, засвідчені заявником або нотаріально;
- заявки на формування кваліфікованих сертифікатів, засвідчені відповідними підписувачами (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 – відокремленого підрозділу (філії, представництва) юридичної особи уповноважений представник надає такі документи:

- заповнений та підписаний договір - у двох примірниках або заповнену та підписану заявником картку приєднання до електронного договору - в одному примірнику;
- оригінал довідки, відомостей чи витягу з ЄДРПОУ, або виписки чи витягу з ЄДР, або копію одного з цих документів, засвідчену нотаріально або підписом керівника та печаткою відокремленого підрозділу (філії, представництва) юридичної особи (за наявності);
- копії паспортів підписувачів або інших документів, що посвідчують особу відповідно до законодавства України, засвідчені відповідними підписувачами або нотаріально;
- копії довідок про присвоєння ідентифікаційних номерів (карток фізичних осіб – платників податку) підписувачів, засвідчені відповідними підписувачами або нотаріально (у випадку, якщо наданий паспорт підписувача не містить значення ІН);
- копії документів про призначення на посаду підписувачів, засвідчені заявником або нотаріально;
- заявки на формування кваліфікованих сертифікатів, засвідчені відповідними підписувачами.

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:

- заповнений та підписаний договір - у двох примірниках або заповнену та підписану картку приєднання до електронного договору - в одному примірнику;
- копія паспорта або іншого документа, який посвідчує особу відповідно до законодавства України, засвідчена підписувачем або нотаріально;
- 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);
- заявки на формування сертифікатів, засвідчені підписувачем.

У разі формування сертифіката електронної печатки ФОП для застосування 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 до комплекту документів надається оригінал виписки чи витягу з ЄДР, або копія одного з цих документів, засвідчена нотаріально або державним реєстратором, або підписом ФОП.

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

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 приміщеннях надавача або відокремлених пунктів реєстрації надавача.

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.

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 на формування, блокування та скасування кваліфікованих сертифікатів відкритих ключів.

Перевірка ідентифікаційних даних заявника, який звертається з заявою в електронній формі, а також законності такого звернення, здійснюється шляхом автентифікації підписувача за результатами перевірки кваліфікованого електронного підпису на заяві та встановлення 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

Цей пункт 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 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

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

4.1.12 Порядок ведення архівів надавача

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

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

В ІТС надавача використовуються особисті та відповідні їм відкриті ключі за такими призначеннями (сферою використання) та з такими параметрами:

- особисті та відповідні їм відкриті ключі надавача для накладення та перевірки електронного підпису на кваліфікованих сертифікатах відкритих ключів підписувачів та СВС зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння", затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі - ДСТУ 4145-2002);
- особисті та відповідні їм відкриті ключі надавача, що використовуються для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;
- особисті та відповідні їм відкриті ключі надавача для накладення та перевірки електронного підпису на даних про статус кваліфікованих сертифікатів відкритих

ключів підписувачів, що визначається в режимі реального часу, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;

- особисті та відповідні їм відкриті ключі серверів обробки запитів, що використовуються для криптографічного захисту повідомлень, які передаються відкритими каналами зв'язку, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;
- особисті та відповідні їм відкриті ключі посадових осіб, що використовуються для автентифікації посадових осіб та криптографічного захисту повідомлень, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;
- особисті та відповідні їм відкриті ключі надавача для накладення та перевірки електронного підпису на кваліфікованих сертифікатах відкритих ключів підписувачів та СВС із використанням іменованої еліптичної кривої NIST P-256 (secp256r1) для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2015 "Електронні підписи й інфраструктури (ESI). Криптографічні комплекти" (далі - ДСТУ ETSI EN 119 312:2015);
- особисті та відповідні їм відкриті ключі надавача, що використовуються для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу із використанням іменованої еліптичної кривої NIST P-256 (secp256r1) для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2015;
- особисті та відповідні їм відкриті ключі надавача для накладення та перевірки електронного підпису на даних про статус кваліфікованих сертифікатів відкритих ключів підписувачів, що визначається в режимі реального часу, із використанням іменованої еліптичної кривої NIST P-256 (secp256r1) для алгоритму ECDSA згідно з ДСТУ ETSI EN 119 312:2015;
- особисті та відповідні їм відкриті ключі надавача для накладення та перевірки електронного підпису на кваліфікованих сертифікатах відкритих ключів підписувачів та СВС з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015;
- особисті та відповідні їм відкриті ключі надавача, що використовуються для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу, з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015;
- особисті та відповідні їм відкриті ключі надавача для накладення та перевірки електронного підпису на даних про статус кваліфікованих сертифікатів відкритих ключів підписувачів, що визначається в режимі реального часу, з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015.

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 та сервера TSP

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

4.1.13.2 Генерація особистих ключів серверів OCSP та серверів обробки запитів ІТС надавача

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

4.1.13.3 Генерація особистих ключів посадових осіб

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

4.1.13.4 Формування кваліфікованих сертифікатів відкритих ключів надавача

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

4.1.13.5 Формування кваліфікованих сертифікатів відкритих ключів серверів ІТС надавача (TSP, OCSP, серверів обробки запитів)

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

4.1.13.6 Формування кваліфікованих сертифікатів відкритих ключів посадових осіб

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

4.1.13.7 Планова заміна ключів надавача

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

4.1.13.8 Планова заміна ключів серверів ІТС надавача (TSP, OCSP, серверів обробки запитів)

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

4.1.13.9 Планова заміна ключів посадових осіб

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

4.1.13.10 Позапланова заміна ключів

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

4.1.13.11 Генерація ключів користувачів

Особистий ключ 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 офісі надавача або його відокремлених пунктів реєстрації;
- у «хмарному» сховищі ключів надавача.

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 та серверів ІТС надавача

4.1.16.1 Порядок зберігання ключових даних та носіїв ключової інформації

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

4.1.16.2 Заходи безпеки під час генерації ключових даних

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

4.1.16.3 Порядок знищення особистих ключів надавача та серверів ІТС надавача

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

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

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

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 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.

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.

4.2.2 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.

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.

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.

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 4.3.

Таблиця 4.3

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 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	+	+	+	Документальне підтвердження
порушення користувачем електронних довірчих послуг істотних умов договору про надання кваліфікованих		+		Документальне підтвердження

Підстави для зміни статусу сертифіката	Скасування	Блокування	Поновлення	Підтвердження підстав
електронних довірчих послуг				

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 4.2 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 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 апаратно-програмних 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.