ПОГОДЖЕНО

Керівник засвідчувального центру НБУ

_____ І.В.Коновалов

“_____”_____ 2022 р.

ЗАТВЕРДЖЕНО: Стефано Бурані, Голова Правління Банку

_____

Олексій Сіраков, директор департаменту управління інформаційною безпекою та безперервністю бізнесу

_____

Реєстраційний номер № 278 від 20.12.2021

РЕГЛАМЕНТ РОБОТИ КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ АТ «ПРАВЕКС БАНК»

Класифікація документу за рівнем безпеки: **відкрита інформація**

Перелік змін:

Версія	Дата видання	Власник	Ключові зміни	Скасовані документи
1.0	20.12.2021	Департамент управління інформаційною безпекою та безперервністю бізнесу	Відсутні.	Відсутні.

Розміщення документу:
https://my.pravex.ua – INTERNAL RULES & REGULATIONS BASE – OPERATIONAL DOCUMENTS – ICT Management & IT Security

Дата набуття чинності:

Структурні підрозділи, які погоджують та яким розсилається документ:

	Список погодження	Список розсилання		Список погодження	Список розсилання
Голова Правління	☐	☐	Департамент управління персоналом та організаційними змінами	☒	☐
Головний бухгалтер	☐	☐	Департамент управління інформаційною безпекою та безперервністю бізнесу	☐	☒
Департамент внутрішнього аудиту	☐	☒	Головне управління роздрібного бізнесу	☐	☐
Департамент юридичної підтримки та генерального секретаріату	☐	☒	Головне управління корпоративного бізнесу	☐	☐
Департамент управління ризиками	☐	☒	Головне фінансове управління	☐	☐
Департамент комплаєнсу та протидії легалізації доходів, отриманих злочинним шляхом	☐	☒	Головне кредитне управління	☐	☐
Відділ зв’язків з громадськістю та маркетингу	☐	☐	Головне операційне управління	☐	☐

ЗМІСТ

ВСТУП

Терміни та скорочення:

Надавач – кваліфікований Надавач електронних довірчих послуг АКЦІОНЕРНОГО ТОВАРИСТВА "ПРАВЕКС БАНК" (далі - Банк), відомості про якого внесені до Довірчого списку за поданням засвідчувального центру;

Клієнт – фізична особа, фізична особа - підприємець, юридична особа, представник юридичної особи або співробітник Банку, який на законних підставах звертається до Надавача з метою отримання кваліфікованих електронних довірчих послуг або якому Надавач надає кваліфіковані електронні довірчі послуги у встановленому цим Регламентом порядку;

особистий ключ Надавача – особистий ключ, який Надавач використовує для надання кваліфікованих електронних довірчих послуг;

ключі серверів Надавача – пари ключів, які Надавач використовує для створення позначки часу (далі – ключі TSP-сервера); пари ключів, які Надавач використовує для надання інформації про статус кваліфікованого сертифіката відкритого ключа за запитом на інтерактивну перевірку статусу (далі – ключі OCSP-сервера); пари ключів, які Надавач використовує для обробки запитів згідно з протоколом Certificate Management Protocol (далі – ключі CMP-сервера);

веб-сайт – офіційний інформаційний ресурс Надавача;

реєстр Надавача – електронна база даних, яка ведеться Надавачем та містить відомості про Клієнтів, а також дані, необхідні для надання довірчих послуг, які надає Надавач;

реєстрація – внесення інформації про Клієнта до реєстру Надавача;

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;

НКІ - Носій ключової інформації;

ОС - Операційна система;

ПЗ - Програмне забезпечення;

РНОКПП - Реєстраційний номер облікової картки платника податків;

ЄДРПОУ - Єдиний державний реєстр підприємств та організацій України;

УНЗР - Унікальний номер запису в ЄДДР;

ЦОД - Центр обробки даних;

СВС – список відкликаних сертифікатів.

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», «Положенні про кваліфікованих Надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру», затвердженому постановою Правління Національного банку України від 19 вересня 2019 року № 116, 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 АТ "ПРАВЕКС БАНК", 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 роботи Надавача розроблений відповідно до вимог Положення про кваліфікованих Надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру, затвердженого постановою Правління Національного банку України від 19 вересня 2019 року № 116, наказу ДССЗЗІ №269 від 14.05.20 «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих Надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації» та вимог законодавства України у сфері електронних довірчих послуг.

Вимоги регламенту є обов’язковими до виконання Надавачем.

Визнання вимог регламенту Клієнтами є обов’язковою умовою та підставою для укладання з ними договору про надання електронних довірчих послуг.

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 чинного законодавства.

Надавач має право в односторонньому порядку вносити зміни та доповнення до Регламенту. Повідомлення про внесення змін та доповнень до Регламенту, а також уточнена редакція Регламенту розміщуються на офіційному веб-сайті Надавача не пізніше ніж за 10 (десять) робочих днів до вступу змін та доповнень у дію.

Якщо Клієнт не згоден із внесеними змінами та доповненнями, він має право припинити використання послуг.

1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО НАДАВАЧА

Повне найменування юридичної особи Надавача: АКЦІОНЕРНЕ ТОВАРИСТВО "ПРАВЕКС БАНК".

Скорочене найменування юридичної особи: АТ "ПРАВЕКС БАНК".

Повне найменування Надавача: КВАЛІФІКОВАНИЙ НАДАВАЧ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ АКЦІОНЕРНОГО ТОВАРИСТВА "ПРАВЕКС БАНК".

Скорочене найменування Надавача: КНЕДП АТ "ПРАВЕКС БАНК".

Код ЄДРПОУ: 14360920.

Юридична адреса Надавача: 01021, Україна, м. Київ, Кловський узвіз, 9/2.

Адреса розміщення головного офісу Надавача: 01021, Україна, м. Київ, Кловський узвіз, 9/2.

Номер телефону, який використовується виключно для блокування/скасування/поновлення і надання інформації про статус сертифікатів відкритих ключів у телефонному режимі: 044-5210418.

Номери телефонів для консультацій: 0 800 500 450 - безкоштовно в межах України.

Електронна адреса офіційного веб-сайту Надавача: https://ca.pravex.com.ua

Адреса електронної пошти головного офісу Надавача: ca@pravex.ua

Режим роботи: з 9:00 до 18:00, з понеділка по п‘ятницю. В святкові та передсвяткові дні режим роботи встановлюється розпорядженням НБУ.

Головний офіс Надавача представлений окремим підрозділом АТ "ПРАВЕКС БАНК", що здійснює надання кваліфікованих електронних довірчих послуг та забезпечує виконання вимог законодавства до Надавачів.

Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені АТ "ПРАВЕКС БАНК".

2 ПЕРЕЛІК ІНФОРМАЦІЇ, ЩО РОЗМІЩУЄТЬСЯ НАДАВАЧЕМ НА ОФІЦІЙНОМУ ВЕБ-САЙТІ

Офіційний інформаційний ресурс Надавача призначено для розміщення на ньому наступної відкритої інформації:

- відомості про Надавача та режим його роботи;
- положення цього Регламенту;
- кваліфіковані сертифікати відкритих ключів Надавача;
- перелік кваліфікованих електронних довірчих послуг, які надає Надавач;
- перелік та форми документів, які подаються для отримання кваліфікованих електронних довірчих послуг;
- відомості про обмеження під час використання кваліфікованих сертифікатів відкритих ключів;
- перелік нормативно-правових актів у сфері електронних довірчих послуг;
- реєстр чинних, блокованих та скасованих сертифікатів ключів та СВС;
- дані про внесення відомостей про Надавача до Довірчого списку;
- дані про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг;
- дані про засоби кваліфікованого електронного підпису чи печатки, які Надавач надає своїм Клієнтам (коли кваліфікована електронна довірча послуга передбачає використання таких засобів);
- дані про порядок перевірки статусу кваліфікованого сертифіката відкритого ключа;
- інша інформація необхідна для використання кваліфікованих електронних довірчих послуг.

На офіційному веб-сайті Надавача також публікується інформація про призупинення обслуговування Клієнтів, про зміну схеми обслуговування Клієнтів у разі перенесення роботи кваліфікованого Надавача до віддаленого резервного пункту та/або виникнення критичних ситуацій, а також інформація про наміри Надавача припинити надання кваліфікованих електронних довірчих послуг.

3 ПЕРЕЛІК КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

Перелік кваліфікованих електронних довірчих послуг, що надаються:

- створення, перевірка та підтвердження кваліфікованого електронного підпису чи печатки;
- формування, перевірка та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;
- формування, перевірка та підтвердження кваліфікованої електронної позначки часу.

Окрім надання кваліфікованих електронних довірчих послуг, Надавач надає консультаційні послуги за зверненням Клієнтів.

Надання вищезазначених послуг здійснюється Надавачем у відповідності до цього Регламенту та на підставі підписаних Договорів.

4 ПЕРЕЛІК ПОСАД ТА ФУНКЦІЇ ПРАЦІВНИКІВ НАДАВАЧА

4.1 Працівники Надавача

Надавач для надання довірчих послуг призначає працівників, які виконують функції:

- керівника Надавача;
- заступника керівника Надавача;
- адміністратора реєстрації;
- адміністратора сертифікації;
- адміністратора безпеки;
- системного адміністратора.

4.2 Керівник Надавача

Керівник Надавача в межах виконання своїх обов'язків:

- здійснює загальне керівництво діяльністю Надавача і контроль за його діяльністю;
- дає доручення, обов’язкові для адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, адміністратора безпеки;
- затверджує розпорядчі акти, інструкції, проектну й експлуатаційну документації, документи, що визначають організаційні, технічні та технологічні умови діяльності кваліфікованого Надавача;
- здійснює представництво та захист інтересів Надавача в сфері кваліфікованих електронних довірчих послуг.

4.3 Заступник керівника Надавача

Заступник керівника Надавача виконує функції керівника Надавача в разі його відсутності або за його письмовим дорученням.

4.4 Адміністратор реєстрації

Адміністратор реєстрації відповідає за ідентифікацію, автентифікацію, верифікацію Клієнтів, надання допомоги під час генерації пар ключів, перевірку документів, наданих Клієнтами.

До завдань адміністратора реєстрації також відносяться:

- перевірка законності звернень про блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів;
- надання Клієнтам консультацій щодо умов та порядку отримання кваліфікованих електронних довірчих послуг.

4.5 Адміністратор сертифікації

Адміністратор сертифікації відповідає за:

- формування кваліфікованих сертифікатів відкритих ключів;
- ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;
- генерацію, створення резервних копій, та використання особистих ключів Надавача;
- збереження особистих ключів Надавача та їх резервних копій.

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

4.6 Адміністратор безпеки

Адміністратор безпеки відповідає за належне функціонування комплексної системи захисту інформації, а також за проведення перевірок дотримання адміністраторами реєстрації, адміністраторами сертифікації, системними адміністраторами вимог документації комплексної системи захисту інформації Надавача.

До завдань адміністратора безпеки також відносяться:

- проектування, розроблення, експлуатація, обслуговування та модернізація комплексної системи захисту інформації інформаційно-телекомунікаційної системи Надавача;
- контроль процесу генерації пар ключів Надавача та створення резервних копій особистих ключів Надавача;
- контроль за зберіганням особистих ключів Надавача та їх резервних копій;
- контроль за зберіганням особистих ключів адміністраторів;
- участь у знищенні особистих ключів Надавача;
- контроль за знищенням особистих ключів адміністраторів;
- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації 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 визначених документацією щодо комплексної системи захисту інформації;
- перевірка та аналіз журналів аудиту подій, що реєструють технічні засоби інформаційно-телекомунікаційної системи Надавача.

Проведення перевірок дотримання адміністраторами реєстрації, адміністраторами сертифікації, системними адміністраторами вимог документації комплексної системи захисту інформації здійснюється адміністратором безпеки один раз на рік.

Забороняється суміщення обов'язків адміністратора безпеки з обов'язками адміністратора реєстрації, адміністратора сертифікації та системного адміністратора. Надавач забезпечує щорічне проходження адміністратором безпеки та системним адміністратором практичних навчань з інформаційної безпеки, що передбачають вивчення нових загроз інформаційної безпеки та реагування на них.

4.7 Системний адміністратор

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;

- забезпечення 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.

5 ПОЛІТИКА СЕРТИФІКАТА ТА ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

5.1 Політика сертифіката

5.1.1 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
Перевірка кваліфікованої електронної печатки	digitalSignature + nonRepudiation
Узгодження ключів шифрування	keyAgreement

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.

5.1.2 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.

5.1.3. Перелік сертифікатів відкритих ключів Надавача

Надавач для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих сертифікатів електронного підпису чи печатки Клієнтам використовує наступні сертифікати відкритих ключів Надавача:

1) кваліфіковані сертифікати відкритих ключів Надавача, сформовані засвідчувальним центром, що використовуються для формування та перевірки кваліфікованих сертифікатів відкритих ключів Клієнтів та списків відкликаних сертифікатів;

2) кваліфіковані сертифікати ключів Надавача, що використовуються для надання інформації про статус кваліфікованих сертифікатів ключів Клієнтів за запитом на інтерактивну перевірку статусу кваліфікованого сертифіката відкритого ключа;

3) кваліфіковані сертифікати відкритих ключів Надавача, сформовані засвідчувальним центром, що використовуються для формування та перевірки електронних позначок часу.

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

Надавач публікує на власному офіційному веб-сайті:

- кваліфіковані сертифікати відкритих ключів засвідчуваного центру;
- кваліфіковані сертифікати відкритих ключів Надавача;
- кваліфіковані сертифікати відкритих ключів Клієнтів Надавача;
- повний та частковий СВС.

Публікація чинних кваліфікованих сертифікатів відкритих ключів

Публікація чинних кваліфікованих сертифікатів відкритих ключів Клієнтів на офіційному веб-сайті Надавача здійснюється одразу після їх формування, за умов перевірки Клієнтом даних, що вносяться до кваліфікованого сертифікату відкритого ключа.

Публікація на офіційному веб-сайті Надавача кваліфікованих сертифікатів відкритих ключів Клієнтів здійснюється за їхньої згоди.

Списки відкликаних сертифікатів

Надавач формує списки відкликаних сертифікатів у вигляді повного та часткового списків.

Повний СВС формується та публікується 1 (один) раз на тиждень та містить інформацію про всі сертифікати ключів, сформовані Надавачем, статус яких був змінений. Доступ до списків відкликаних сертифікатів забезпечується цілодобово.

Частковий СВС формується та публікується не рідше одного разу на дві години та містить інформацію про всі кваліфіковані сертифікати відкритих ключів, статус яких був змінений в інтервалі між часом випуску останнього повного СВС та часом формування поточного часткового СВС.

Публікація кваліфікованих сертифікатів відкритих Надавача

Кваліфіковані сертифікати відкритих власних ключів Надавача та кваліфіковані сертифікати відкритих ключів TSP-сервера публікуються на офіційному веб-сайті Надавача не пізніше ніж наступного робочого дня після їх отримання від засвідчувального центру.

Кваліфіковані сертифікати відкритих ключів OCSP-серверів та CMP-серверів Надавача публікуються на офіційному веб-сайті Надавача відразу після їх формування Надавачем.

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

Для формування кваліфікованих сертифікатів відкритих ключів використовуються запити на формування сертифікатів відкритих ключів підпису та шифрування, які створюються в процесі генерації особистого та відкритого ключів.

Підтвердження володіння Клієнтом особистим ключем та його відповідність відкритому ключу здійснюється адміністратором реєстрації без розкриття особистого ключа Клієнта, шляхом перевірки удосконаленого підпису чи печатки на запиті за допомогою відкритого ключа, що міститься у запиті.

5.1.6 Умови ідентифікації та верифікації Клієнта

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.

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 Клієнта, що звернувся до Надавача для отримання кваліфікованих електронних довірчих послуг, Надавач вимагає разом із заявою надати, а Клієнт 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 Клієнта 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 Клієнтів інші документи, передбачені законодавством.

Для підтвердження належного проведення процедури встановлення Клієнта, Надавач забезпечує зберігання заяв на формування або зміну статусу кваліфікованих сертифікатів відкритих ключів та копій документів, які надавались Клієнтами під час ідентифікації. Копії таких документів зберігаються в паперовому вигляді в архівних приміщенням 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 Клієнта, засвідчуються за правилами, наведеними у Таблиці 4

Таблиця 4

Форма документа	Засвідчення з боку Клієнта		Засвідчення з боку Надавача (адміністратора реєстрації)	
	Тип підпису	Черга засвідчення	Тип підпису	Черга засвідчення
Паперова	Власноручний підпис	Перша	Штамп адміністратора реєстрації на паперових документах Кваліфікований електронний підпис адміністратора реєстрації в підсистемі створення облікових записів Клієнтів	Друга
Електронна	Кваліфікований електронний підпис	Перша	Кваліфікований електронний підпис адміністратора	Друга

			реєстрації на електронному документі Кваліфікований електронний підпис адміністратора реєстрації в підсистемі створення облікових записів Клієнтів	

Засвідчення Надавачем заяв та копій документів без завершення встановлення особи Клієнта та без належного засвідчення ним документів не допускається.

Під час встановлення особи Надавач може використовувати засоби фотофіксації факту пред'явлення Клієнтом документів, що посвідчують особу. Збереження фотодокументів в ІТС Надавача здійснюється після їх засвідчення шляхом створення кваліфікованого електронного підпису адміністратора реєстрації.

5.1.7 Механізм автентифікації Клієнтів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований Надавачем

Автентифікація Клієнтів, 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.

Перевірка ідентифікаційних даних Клієнта, 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.

Поданням такої заяви Клієнт повинен засвідчити незмінність ідентифікаційних даних, внесених до кваліфікованого сертифіката відкритого ключа з моменту формування сертифіката до моменту створення кваліфікованого електронного підпису на заяві.

5.1.8 Механізм ідентифікації, автентифікації, верифікації Клієнтів під час оброблення заяв на блокування, скасування або поновлення кваліфікованого сертифіката ключа

Перелік та опис механізмів ідентифікації, автентифікації, верифікації Клієнтів під час оброблення заяв на блокування, скасування або поновлення кваліфікованого сертифіката 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 Клієнтом 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 Клієнтів, 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 к, 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

5.1.9 Опис фізичного середовища

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

Територіально спеціальне приміщення ІТС Надавача розміщується у ЦОД за адресою: м. Київ, вул. Північно-Сирецька 1-3, у екранованому приміщенні (далі – спеціальне приміщення).

Межа контрольованої зони будівлі ЦОД встановлена по периметру зовнішніх стін та внутрішнього двору будівлі, перекриттям приміщень та даху будинку. Екроване приміщення розташоване усередині контрольованої зони.

Режим доступу до спеціального приміщення визначається наказом Надавача. Доступ співробітникам Надавача до спеціального приміщення надається згідно з їх службовими обов'язками.

Безконтрольний доступ сторонніх осіб до апаратури та обладнання ІТС Надавача в робочий та неробочий час виключений.

Вхід до ЦОД здійснюється через рамку для блокування проходу (шлюзову камеру) обладнаною комп’ютеризованою системою доступу з використанням ідентифікаційних карток. Дозвіл на доступ в ЦОД здійснюється не тільки апаратними засобами системи контролю доступу, а й участю представника охорони, який ідентифікує особу і підтверджує можливість її доступу на територію ЦОД.

Вхід до спеціального приміщення обладнано подвійними екранованими дверима з механічними та електричними замками, інтегрованими до загальної системи контролю доступу, вікна в екранованому приміщенні відсутні.

Реєстрація доступу (входу) до екранованого приміщення здійснюється у електронному журналі системи контролю доступу, який зберігається у ЦОД.

Стіни, підлога та стеля екранованого приміщення збудовані з капітальних негорючих матеріалів, стійких до проникнення зі зломом.

Екранування приміщення виконано з використанням екранованої кабіни, що являє собою збірну конструкцію, виконану із уніфікованих панелей, для протидії побічним електромагнітним випромінюванням та зовнішніх руйнівних електричних сигналів, а також з використанням спеціальних фільтрів для введення систем життєзабезпечення.

Спеціальне приміщення обладнане засобами і системами пожежної та охоронної сигналізації, системами пожежогасіння, кондиціювання та вентиляції для підтримки нормальних кліматичних умов експлуатації технічних засобів ІТС Надавача.

Електроживлення технічних засобів ІТС Надавача забезпечується використанням джерел безперебійного живлення та резервних дизельних генераторів. Заземлення технічних засобів екранованого приміщення виконано у вигляді окремого контуру.

Дротова мережа електроживлення технічних засобів ІТС Надавача обслуговується за нормами Особливої групи І категорії, підключена до окремого електричного щита всередині екранованого приміщення. До екранованого приміщення подаються два вводи електроживлення, а система гарантованого електроживлення забезпечує наявність електроживлення якнайменше на одному вводі. Живлення ЦОД здійснюється від двох незалежних трансформаторних підстанцій, які розташовані поза межами контрольованої зони.

Ланцюги охоронної сигналізації підключені до пультів сигналізації в приміщенні чергової зміни диспетчерів ЦОД. Ланцюги датчиків протипожежної сигналізації підключені до пультів сигналізації в приміщенні чергової зміни диспетчерів ЦОД та міського пульту пожежної сигналізації.

5.1.10 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 в межах організації з урахуванням режиму роботи Надавача передбачає дисциплінарні стягнення, адміністративну та кримінальну відповідальність, передбачені:

- 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.

5.1.11 Порядок ведення журналів аудиту подій

Адміністратор реєстрації, адміністратор сертифікації, системний адміністратор мають право переглядати журнали аудиту подій, пов'язані з виконанням їх функціональних обов'язків.

Надавач забезпечує ведення журналів аудиту подій, в яких реєструються події таких типів:

– спроби створення, знищення, встановлення паролів, зміни прав доступу в ІТС Надавача;

– заміни програмного забезпечення, технічних засобів інформаційно-телекомунікаційної системи Надавача;

– технічне обслуговування інформаційно-телекомунікаційної системи Надавача;

– генерація, використання, знищення особистих ключів Надавача;

– формування, блокування, скасування та поновлення кваліфікованих сертифікатів відкритих ключів, формування СВС;

– спроби несанкціонованого доступу до інформаційно-телекомунікаційної системи Надавача;

– надання доступу адміністраторам до інформаційно-телекомунікаційної системи Надавача;

– збої в роботі інформаційно-телекомунікаційної системи Надавача.

Адміністратор безпеки зобов'язаний вести журнали обліку, передбачені документацією на комплексну систему захисту інформації ІТС Надавача.

Записи в журналах аудиту подій та журналах обліку повинні містити дату та час події, а також ідентифікувати суб'єкта, що здійснив або ініціював подію. Час, що використовується в журналах аудиту подій в електронній формі, повинен бути синхронізований із Всесвітнім координованим часом із точністю до секунди.

Надавач забезпечує захист журналів аудиту подій від неавторизованого перегляду, несанкціонованої модифікації та від знищення.

Адміністратор реєстрації, адміністратор сертифікації, системний адміністратор мають право переглядати журнали аудиту подій, пов'язані з виконанням їх функціональних обов'язків.

Керівник Надавача, заступник керівника Надавача, адміністратор безпеки мають право переглядати всі журнали аудиту подій, які ведуться у Надавача, та всі журнали обліку, передбачені документацією на комплексну систему захисту інформації ІТС Надавача.

Адміністратор реєстрації, адміністратор сертифікації, системний адміністратор зобов'язані:

– переглядати журнали аудиту подій не рідше одного разу на місяць;

– повідомляти адміністратора безпеки про наявність несанкціонованої модифікації в ІТС Надавача, виявлену під час перегляду журналів аудиту подій. Адміністратор безпеки зобов'язаний переглядати журнали аудиту подій не рідше одного разу на тиждень.

Надавач забезпечує зберігання протягом п’яти років з моменту внесення останнього запису:

– журналів аудиту подій;

– журналів обліку, передбачених документацією на комплексну систему захисту інформації ІТС Надавача.

5.1.12 Порядок ведення, збереження, резервування, відновлення, захисту даних, пов’язаних із формуванням та обслуговуванням Надавачем кваліфікованих сертифікатів відкритих ключів

Надавач забезпечує зберігання документованої інформації (документів), на підставі яких Клієнтам надавалися кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані кваліфіковані сертифікати відкритих ключів, усі сформовані кваліфіковані сертифікати відкритих ключів, а також СВС протягом строків, встановлених Правилами застосування переліку документів, що утворюються в діяльності Національного банку України та банків України, затвердженими постановою Правління Національного банку України від 27 листопада 2018 року № 130 (зі змінами), до передавання на архівне зберігання.

Надавач зобов’язаний створити систему резервування та відновлення функціонування інформаційно-телекомунікаційної системи Надавача, яка має забезпечити резервування на основних майданчиках та у віддаленому резервному пункті інформації, із забезпеченням її захисту від несанкціонованого доступу.

Види документів та даних, що підлягають зберіганню, строки зберігання, механізм та порядок зберігання і захисту даних наведено у Таблиці 6.

Таблиця 6

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 адміністраторів Надавача	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
Журнали аудиту подій ІТС Надавача	Паперова	≥ 5 років	Сховище (сейф)
	Електронна	≥ 5 років	Автоматичне резервне копіювання засобами ІТС Надавача та ручне архівне копіювання на окремі носії інформації
Укладені договори про надання послуг	Паперова	Постійно	Автоматичне резервне копіювання засобами ІТС Надавача та ручне архівне копіювання на окремі носії інформації
	Електронна	Постійно	Автоматичне резервне копіювання засобами ІТС Надавача та ручне архівне копіювання на окремі носії інформації
Документи та копії документів, що використовуються під час реєстрації Клієнтів	Паперова	Постійно	Архівне приміщення Надавача
	Електронна	Постійно	Автоматичне резервне копіювання засобами ІТС Надавача та ручне архівне копіювання на окремі носії інформації
Заяви на формування кваліфікованих сертифікатів відкритих ключів	Паперова	Постійно	Архівне приміщення Надавача
	Електронна	Постійно	Автоматичне резервне копіювання засобами ІТС Надавача та ручне архівне копіювання на окремі носії інформації
Заяви на блокування кваліфікованих сертифікатів відкритих ключів	Паперова	Постійно	Архівне приміщення Надавача
	Електронна	Постійно	Автоматичне резервне копіювання засобами ІТС Надавача та ручне архівне копіювання на окремі носії інформації
Заяви на скасування кваліфікованих сертифікатів відкритих ключів	Паперова	Постійно	Архівне приміщення Надавача
Заяви на поновлення кваліфікованих сертифікатів відкритих ключів	Паперова	Постійно	Архівне приміщення Надавача

У разі припинення діяльності Надавача всі документи, на підставі яких підписувачам надавалися послуги електронного цифрового підпису/електронні довірчі послуги/кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані сертифікати відкритих ключів (у тому числі посилені та кваліфіковані) - передаються до Засвідчувального центру Національного банку України.

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, а другий – в опечатаному вигляді зберігається у сховищі (сейфі) керівника 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. 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 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 зберіганню.

5.1.13 Порядок та умови генерації, зберігання, використання пар ключів кваліфікованого Надавача

Цей розділ регламенту не входить до обсягу положень, визначених Надавачем для ознайомлення Клієнтами, окрім положень, що стосується опису процесу, порядку та умови використання пар ключів Клієнтів.

Генерація особистого ключа Надавача виконується у засобі кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроєм, що забезпечує захист записаних даних від несанкціонованого доступу (далі – захищений носій). Особисті ключі Надавача генеруються, зберігаються, використовуються виключно у захищених носіях.

Захищені носії, в яких зберігаються та використовуються особисті ключі Надавача, розташовуються у приміщеннях, що відповідають вимогам Правил з технічного захисту

інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджених постановою Правління Національного банку України від 04 липня 2007 року № 243, зареєстрованих у Міністерстві юстиції України 17 серпня 2007 року за № 955/14222.

Захищені носії, в яких зберігаються резервні копії особистих ключів Надавача, зберігаються із забезпеченням їх захисту від несанкціонованого доступу.

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

Надавач використовує наступні пари ключів:
- Особистий ключ Надавача;
- Особистий ключ TSP сервера;
- Особистий ключ OCSP сервера;
- Особистий ключ CMP сервера;
- Особисті ключі адміністраторів реєстрації.

Особистий ключ Надавача використовується виключно для формування СВС, кваліфікованих сертифікатів відкритих ключів OCSP та CMP серверів, кваліфікованих сертифікатів відкритих ключів Клієнтів.

Особистий ключ TSP-сервера використовується виключно під час формування відповіді на запит на позначку часу.

Особистий ключ OCSP-сервера використовується виключно під час формування відповіді на запит про статус кваліфікованого сертифіката в режимі реального часу.

Особистий ключ CMP-сервера використовується для обробки запитів на формування, блокування, скасування кваліфікованих сертифікатів відкритих ключів, отримання та перевірки власних сертифікатів Клієнтів та інше.

Особисті ключів адміністраторів реєстрації використовуються виключно для їх автентифікації в ПТК та для забезпечення конфіденційності даних, які обробляються ними.

Адміністратор сертифікації за участю адміністратора безпеки здійснює генерацію пар ключів Надавача з такими параметрами:

- для підпису кваліфікованих сертифікатів відкритих ключів та СВС з довжиною ключа 257 біт згідно з ДСТУ 4145-2002;
- для електронного підпису обробки повідомлень CMP-серверу з довжиною ключа 257 біт згідно з ДСТУ 4145-2002;
- для протоколу розподілу ключів обробки повідомлень CMP-серверу з довжиною ключа 431 біт згідно з ДСТУ 4145-2002;
- для підпису OCSP-відповідей з довжиною ключа 257 біт згідно з ДСТУ 4145-2002;
- для формування позначок часу з довжиною ключа 257 біт згідно з ДСТУ 4145-2002.

Особисті ключі Надавача та ключі серверів Надавача у програмно-технічному комплексі захищаються на паролях шляхом вироблення імітовставки за ДСТУ ГОСТ 28147:2009 та зашифрування в режимі простої заміни ДСТУ ГОСТ 28147:2009 на ключах, які отримані шляхом хешування строки пароля за ГОСТ 34.311-95. Паролі повинні відповідати наступним вимогам:

- алфавіт символів пароля – англійські букви “a” – “z”, “A” – “Z”, цифри “0” – “9” та символи “-”, “+” (потужність алфавіту – 2^6, 6 біт/символ);

- довжина пароля – мінімальна 8, максимальна 42 символи (48-252 біт, потужність системи паролювання $2^{46} – 2^{252}$);
- обмеження до появлення символів в паролі – не допускається введення більш ніж 2-ох символів, що розташовані поруч на розкладці клавіатури робочої станції, не допускається введення більш ніж 2-ох однакових символів на всій довжині пароля.

Знищення особистих ключів Надавача, його серверів та посадових осіб здійснюється згідно з експлуатаційною документацією на відповідні захищені носії, у яких вони зберігалися та використовувалися. Процедура знищення особистих ключів забезпечує неможливість відновлення ключів після знищення.

Факти генерації та знищення особистих ключів, а також їх резервних копій заносяться до журналу обліку ключових даних. За фактом знищення особистих ключів складаються акти.

5.1.14 Порядок та умови резервного копіювання особистого ключа Надавача, збереження, доступу та використання резервних копій

Резервні копії особистих ключів Надавача зберігаються у захищених носіях.

Адміністратор сертифікації створює дві резервні копії особистих ключів Надавача за участю адміністратора безпеки. Адміністратор безпеки реєструє факти створення резервних копій особистих ключів Надавача у відповідному журналі обліку. Захищені носії з резервними копіями вкладаються в паперові конверти або портативні металеві сейфи, які замикаються на ключ та опломбовується. На конверті/портативному сейфі зазначається дата створення резервних копій, прізвище та ім’я адміністратора сертифікації та номера захищений носіїв з резервними копіями.

Один конверт чи сейф зберігається в основному приміщенні Надавача, а другий – у віддаленому резервному пункті.

У разі необхідності відновити особистий ключ Надавача з резервної копії, адміністратором сертифікації, під наглядом адміністратора безпеки відкривається конверт/сейф з захищеними носіями резервних копій особистих ключів Надавача, про що адміністратор безпеки робить запис у відповідному журналі.

Особистий ключ Надавача та всі його резервні копії після закінчення строку дії кваліфікованого сертифіката відкритого ключа Надавача знищуються способом, що унеможливлює їх відновлення. Адміністратор сертифікації здійснює знищення особистих ключів Надавача та їх резервних копій за участю адміністратора безпеки.

5.1.15 Порядок та умови генерації пар ключів Клієнтів, механізм отримання Клієнтом особистого ключа в результаті надання кваліфікованої електронної довірчої послуги Надавачем, механізм надання Клієнтом запиту на формування кваліфікованого сертифіката відкритого ключа

Генерація особистих та відкритих ключів Клієнта здійснюється ним особисто в кабінеті Клієнта Надавача з використанням засобів кваліфікованого електронного підпису чи печатки. Відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе Клієнт.

В процесі генерації ключових пар Клієнта збереження його особистих ключів здійснюється у апаратно-програмних засобах кваліфікованого електронного підпису чи печатки Клієнта, спеціально призначених для генерації та зберігання особистих ключів або у апаратно-програмних засобах кваліфікованого електронного підпису чи печатки, які є

частиною програмно-технічного комплексу Надавача та мають відповідні експертні висновки в сфері криптографічного та технічного захисту інформації.

Засіб кваліфікованого електронного підпису чи печатки за допомогою відповідного особистого ключа створює самопідписані запити на формування кваліфікованих сертифікатів відкритих ключів підпису та шифрування, які містять відкриті ключі Клієнта та додаткову інформацію для формування кваліфікованих сертифікатів відкритих ключів у Надавача.

Після генерації пар ключів Клієнта у апаратно-програмних засобах кваліфікованого електронного підпису чи печатки, які є частиною ПТК Надавача та формування Надавачем відповідного кваліфікованого сертифіката відкритого ключа, особистий ключ стає доступний Клієнту для використання.

Передача самопідписаних запитів для формування кваліфікованих сертифікатів відкритих ключів здійснюється в кабінеті Клієнта Надавача автоматично по завершенні процедури генерації особистих та відкритих ключів Клієнта.

Строк дії особистого ключа Клієнта становить не більше 2 років. Початком строку дії особистого ключа Клієнта вважається дата та час формування кваліфікованого сертифіката відкритого ключа.

5.2 Положення сертифікаційних практик

5.2.1 Процес подання запиту на формування кваліфікованого сертифіката відкритого ключа

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

Запит на формування кваліфікованого сертифіката відкритого ключа приймається в обробку після приймання та реєстрації заяви на формування кваліфікованого сертифіката, встановлення (ідентифікації) особи Клієнта та підтвердження володіння Клієнтом 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 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 Клієнта та підтвердження володіння Клієнтом 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 формування кваліфікованого сертифіката, становить не більше однієї години.

5.2.2 Порядок надання сформованого кваліфікованого сертифіката відкритого ключа Клієнту

Надання сформованого кваліфікованого сертифіката відкритого ключа Клієнту 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 Клієнтом;
- шляхом публікації сформованого кваліфікованого сертифіката відкритого ключа на офіційному веб-сайті Надавача.

Клієнт повинен перевірити свої ідентифікаційні дані, внесені Надавачем до кваліфікованого сертифіката відкритого ключа. Надавач повинен надавати відповідні консультації щодо проведення такої перевірки. Клієнт 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 Клієнтом невідповідності ідентифікаційних даних, внесених Надавачем до кваліфікованого сертифіката відкритого ключа, Клієнт звертається до Надавача для скасування кваліфікованого сертифіката відкритого ключа та формування нового сертифіката у порядку, встановленому цим регламентом.

5.2.3 Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа Клієнта на офіційному веб-сайті Надавача

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

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

5.2.4 Умови використання кваліфікованого сертифіката відкритого ключа Клієнта та його особистого ключа

Клієнти 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 Клієнтом 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 Клієнта до інформації, підробка електронних документів, матеріальні та репутаційні втрати.

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

5.2.5 Процедура подачі запиту на формування кваліфікованого сертифіката відкритого ключа для Клієнтів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований Надавачем

Електронний запит на формування нового кваліфікованого сертифіката відкритого ключа для Клієнтів, які мають чинний кваліфікований сертифікат відкритого ключа, попередньо сформований Надавачем, подається засобами кваліфікованого електронного підпису чи печатки разом із електронною заявою про формування нового кваліфікованого сертифіката відкритого ключа.

При цьому, 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 Клієнта;
- автоматичне формування заяви про формування нового кваліфікованого сертифіката відкритого ключа із використанням ідентифікаційних даних, внесених до попереднього сертифіката;
- створення кваліфікованого електронного підпису до цієї заяви із використанням попереднього особистого ключа;
- генерацію нової ключової пари та формування запиту на формування кваліфікованого сертифіката відкритого ключа у форматі PKCS#10;
- 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.

5.2.6 Порядок скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа

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

Перелік підстав для зміни статусу кваліфікованого сертифіката із зазначенням суб’єктів подання запитів на зміну статусу та форм підтвердження підстав наведено у Таблиці 7.

Таблиця 7

Підстави для зміни статусу сертифіката	Скасу-вання	Блоку-вання	Поновлення	Підтвердження підстав
подання Клієнтом заяви	+	+	+	Заява Клієнта
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 Клієнта	+			Документальне або технічне (отримання інформації в електронному вигляді з ЄДР) підтвердження
надання Клієнтом недостовірних ідентифікаційних даних	+			Документальне підтвердження
факт компрометації особистого ключа Клієнта, виявлений контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг	+			Документальне підтвердження
повідомлення Клієнтом або контролюючим органом про підозру в компрометації особистого ключа Клієнта електронних довірчих послуг		+		Заява Клієнта або документальне підтвердження
повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа Клієнта контролюючим органом, який раніше повідомив про цю підозру			+	документальне підтвердження
набрання законної сили рішенням суду	+	+	+	Документальне підтвердження
порушення Клієнтом 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-Клієнта.

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

Надавач здійснює прийом та перевірку заяв Клієнтів про скасування, блокування та поновлення їх кваліфікованих сертифікатів відкритих ключів 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 кваліфікованого сертифіката та здійснення відповідної перевірки достовірності документальних повідомлень та автентифікації Клієнтів.

5.2.7 Порядок та умови надання інформації про статус кваліфікованих сертифікатів відкритих ключів, сформованих Надавачем

Періодичність формування СВС та строки його дії

Надавач формує СВС у вигляді повного та часткового списків. Повний список відкликаних кваліфікованих сертифікатів відкритих ключів формується та публікується 1 раз на тиждень та містить інформацію про всі кваліфіковані сертифікати відкритих ключів, які були сформовані Надавачем, статус яких був змінений.

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

Можливість та умови надання інформації про статус кваліфікованого сертифіката відкритого ключа в режимі реального часу

Розповсюдження інформації про статус кваліфікованих сертифікатів електронного підпису чи печатки Клієнтів здійснюється також шляхом створення можливості перевірки статусу кваліфікованого сертифіката електронного підпису чи печатки Клієнта в режимі реального часу через телекомунікаційні мережі загального користування із використанням протоколу OCSP.

Посилання на сервіс перевірки статусу кваліфікованого сертифіката електронного підпису чи печатки Клієнта в режимі реального часу вносяться до кваліфікованих сертифікатів відкритих ключів Клієнтів.

5.2.8 Строки дії кваліфікованих сертифікатів відкритих ключів, сформованих кваліфікованим Надавачем

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

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

Строк дії кваліфікованих сертифікатів відкритих ключів OCSP-сервера Надавача не може перевищувати п’яти років.

Строк дії кваліфікованих сертифікатів відкритих ключів CMP-сервера Надавача не може перевищувати п’яти років.

По закінченні строку дії кваліфікованого сертифіката, такий кваліфікований сертифікат відкритого ключа вважається нечинним та вилучається з публікації на офіційному веб-сайті Надавача.

Надавач зберігає всі сформовані ним кваліфіковані сертифікати відкритих ключів та пов’язані з ними СВС безстроково. За запитом Клієнта Надавач надає доступ до необхідного кваліфікованого сертифіката відкритого ключа та пов’язаних з ним СВС.

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

6.1 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 криптографічного захисту інформації.

Надання Надавачем засобів кваліфікованого електронного підпису чи печатки у вигляді апаратно-програмних засобів 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, здійснюється на договірних засадах та може здійснюватися шляхом передачі цих засобів на носіях інформації безпосередньо Клієнту або шляхом надання доступу через офіційний веб-сайт Надавача.

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

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

- формування кваліфікованої електронної позначки часу;
- передачу кваліфікованої електронної позначки часу Клієнту.

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.

Формування та перевірка кваліфікованої електронної позначки часу здійснюється з використанням засобів кваліфікованого електронного підпису чи печатки.

Перевірка кваліфікованої електронної позначки часу може проводитися будь-яким користувачем з метою отримання інформації про чинність кваліфікованої електронної позначки часу.

Під час перевірки та підтвердження кваліфікованої електронної позначки часу особа, що проводить перевірку, вчиняє такі дії:

1) отримує з кваліфікованої електронної позначки часу інформацію, що містить ідентифікаційні дані особи, які дають змогу однозначно встановити Надавача;
2) перевіряє кваліфікований електронний підпис, накладений на кваліфіковану електронну позначку часу за допомогою чинного (на момент формування кваліфікованої електронної позначки часу) кваліфікованого сертифіката Надавача;
3) перевіряє відповідність кваліфікованої електронної позначки часу та електронних даних, до яких вона додана.

Кваліфікована електронна позначка часу вважається недійсною у разі:

1) недотримання вимоги щодо точності часу у ПТК Надавача;

2) використання скасованого або блокованого кваліфікованого сертифіката Надавача на момент формування кваліфікованої електронної позначки часу.

Кваліфікована електронна позначка часу повинна забезпечувати зв'язок дати і часу з електронними даними в такий спосіб, що цілком виключає можливість непомітної зміни електронних даних;

6.3 Припинення діяльності Надавача

У разі припинення надання кваліфікованих електронних довірчих послуг Надавач зобов'язаний передати засвідчувальному центру документовану інформацію (документи, на підставі яких Клієнтам надавалися кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані кваліфіковані сертифікати відкритих ключів, усі сформовані кваліфіковані сертифікати відкритих ключів, а також реєстри сформованих кваліфікованих сертифікатів відкритих ключів) у порядку, визначеному Правилами передавання документованої інформації до засвідчувального центру кваліфікованими Надавачами електронних довірчих послуг, відомості про яких унесені до Довірчого списку за поданням засвідчувального центру, затвердженими Постановою Правління Національного банку України від 17.02.2020 № 19.

6.4 Необхідні вимоги до процедур

Надавач встановлює вимоги до процедур з управління ризиками, персоналом, операційною безпекою, інцидентами, доказами та архівами, поводження з персональними даними Клієнтів, процедур встановлення Клієнта, опису фізичного середовища.

Зазначені вимоги затверджуються як окремий документ Надавача.