monobank | Universal Bank

«ПОГОДЖЕНО»

Керівник засвідчувального центру

_____ Олександр СКОМАРОВСЬКИЙ

«__» _____ 2024 р.

«ЗАТВЕРДЖЕНО»

Голова Правління

АТ «УНІВЕРСАЛ БАНК»

_____ Ірина СТАРОМІНСЬКА

«20» 11 2024 р.

РЕГЛАМЕНТ

Назва	:	**Регламент роботи кваліфікованого надавача електронних довірчих послуг monobank | Universal Bank АТ «УНІВЕРСАЛ БАНК»**
Відповідальний підрозділ	:	Відділ кваліфікованого надавача електронних довірчих послуг Департаменту інформаційної безпеки
Мета	:	Регламент описує порядок та умови надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем електронних довірчих послуг
Категорія	:	Відкрита інформація
Версія	:	1.0.

«ПОГОДЖЕНО»

Керівник відділу кваліфікованого надавача електронних довірчих послуг
АТ «УНІВЕРСАЛ БАНК»

_____ Віталій КАРЛАШ

«08» 11 2024 р.

м. Київ – 2024

ДОКУМЕНТ СЕД НБУ АСКОД

Підписувач Скомаровський Олександр Анатолійович
Сертифікат 36186A0FEAAD76B20400000023030000E88D0000
Дійсний до:09.08.2025 12:12:39

Національний банк України

56-0014/84759
від 08.11.2024 12:05

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Терміни та скорочення:

1.1.1. У цьому Регламенті терміни та скорочення вживаються у наступних значеннях:

Аудитор системи	–	посада, передбачена у Надавача для здійснення функцій, визначених пунктом 5.7 цього Регламенту, у складі Відділу КНЕДП Департаменту інформаційної безпеки Банку, як підрозділу 1 лінії захисту та не передбачає виконання функцій внутрішнього аудиту у відповідності до вимог Положення НБУ № 311, у тому числі в частині виконання функцій, передбачених вимогами п.47 Положення НБУ № 116 в частині проведення щорічного аудиту;
Банк	–	АКЦІОНЕРНЕ ТОВАРИСТВО «УНІВЕРСАЛ БАНК» (далі – Банк, АТ «УНІВЕРСАЛ БАНК»);
Веб-сайт Надавача	–	Офіційний інформаційний ресурс Надавача https://ca.monobank.ua;
ЄДДР	–	Єдиний державний демографічний реєстр;
ЄДР	–	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань;
ЄДРПОУ	–	Єдиний державний реєстр підприємств та організацій України;
ІКС	–	інформаційно-комунікаційна система;
КЗІ	–	криптографічний захист інформації;
Клієнт	–	фізична особа, фізична особа - підприємець, юридична особа, представник юридичної особи або працівник Банку, який на законних підставах звертається до Надавача з метою отримання кваліфікованих електронних довірчих послуг або якому Надавач надає кваліфіковані електронні довірчі послуги у порядку встановленому цим Регламентом (далі – Клієнт, користувач);
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 про статус кваліфікованого сертифіката в режимі реального часу в базі даних Надавача (далі – ключі OCSP-сервера);
Надавач	–	кваліфікований надавач електронних довірчих послуг monobank | Universal Bank АТ «УНІВЕРСАЛ БАНК», відомості про якого внесені до Довірчого списку за поданням засвідчувального центру;
Особистий ключ Надавача	–	особистий ключ, який Надавач використовує для надання кваліфікованих електронних довірчих послуг;
ПЗ	–	програмне забезпечення;
ПТК	–	програмно-технічний комплекс;
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;
РНОКПП	–	реєстраційний номер облікової картки платника податків;
СВС	–	список відкликаних сертифікатів;
СУІБ	–	система управління інформаційною безпекою;
ТЗІ	–	технічний захист інформації;
УНЗР	–	унікальний номер запису в ЄДДР.

1.1.2. У цьому Регламенті терміни: автентифікація, багатофакторна автентифікація, блокування сертифіката відкритого ключа, веб-сайт, відкритий ключ (дані для підтвердження електронного підпису чи електронної печатки), відокремлений пункт реєстрації (далі – ВПР), Довірчий список, документована інформація, електронна довірча послуга, електронна ідентифікація, електронна печатка, електронна позначка часу, електронна послуга, електронний підпис, електронні дані, засвідчення чинності відкритого ключа, засіб електронного підпису чи печатки, засіб електронної ідентифікації, засіб кваліфікованого електронного підпису чи печатки, ідентифікаційні дані особи, ідентифікація особи, кваліфікована електронна печатка, кваліфікована електронна позначка часу, кваліфікований електронний підпис, кваліфікований надавач

електронних довірчих послуг, кваліфікований сертифікат електронного підпису, кваліфікований сертифікат електронної печатки, компрометація засобу електронної ідентифікації, компрометація особистого ключа, користувачі електронних довірчих послуг, користувачі послуг електронної ідентифікації, надавач електронних довірчих послуг, надавач послуг електронної ідентифікації, орган з оцінки відповідності, особистий ключ (дані для створення електронного підпису чи печатки), пара ключів, підтвердження електронного підпису чи печатки, підтвердження електронної ідентифікації, підписувач, поновлення сертифіката відкритого ключа, послуга електронної ідентифікації, ПТК, що використовується для надання електронних довірчих послуг, реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів, сертифікат електронного підпису, сертифікат електронної печатки, скасування сертифіката відкритого ключа, створювач електронної печатки, схема електронної ідентифікації, технологічна нейтральність технічних рішень, удосконалена електронна печатка, удосконалений електронний підпис, що базується на кваліфікованому сертифікаті електронного підпису, фактор автентифікації вживаються у значеннях, наведених у Законі України «Про електронну ідентифікацію та електронні довірчі послуги» (назва із змінами, внесеними згідно із Законом України від 16.12.2020 № 1089-IX).

1.1.3. Інші терміни в цьому Регламенті вживаються у значеннях, наведених у Цивільному кодексі України, Положенні про кваліфікованих надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру, затвердженому постановою Правління Національного банку України від 19.09.2019 № 116 (із змінами)(далі – Положення про КНЕДП), Вимогах до надавачів послуг електронної ідентифікації та електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 28.06.2024 № 764 (далі – Вимоги до надавачів), інших нормативно-правових актах в сфері електронних довірчих послуг, кіберзахисту, КЗІ та ТЗІ.

1.2. Статус цього Регламенту

1.2.1. Цей Регламент роботи кваліфікованого надавача електронних довірчих послуг monobank | Universal Bank АТ «УНІВЕРСАЛ БАНК» (далі – цей Регламент) є документом Надавача, що визначає організаційно-методологічні, технічні та технологічні умови діяльності Надавача під час надання кваліфікованих електронних довірчих послуг, включаючи політику сертифіката та положення сертифікаційних практик. Надавач має право надавати електронні довірчі послуги та кваліфіковані електронні довірчі послуги.

1.2.2. Цей Регламент розроблено відповідно до вимог:

- Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (Назва Закону в редакції Закону № 2801-IX від 01.12.2022) (далі – Закон);
- Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення»;
- Положення про кваліфікованих надавачів електронних довірчих послуг, унесених до Довірчого списку за поданням засвідчувального центру, затвердженого постановою Правління Національного банку України від 19.09.2019 № 116, зі змінами та доповненнями;
- Вимог до надавачів послуг електронної ідентифікації та електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 28.06.2024 № 764;
- Переліку документів та електронних даних, отриманих у зв’язку з наданням електронних довірчих послуг, що підлягають постійному зберіганню, затвердженого постановою Кабінету Міністрів України від 23.07.2024 № 842;
- Порядку передачі обслуговування користувачів електронних довірчих послуг, з якими кваліфікований надавач електронних довірчих послуг, що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, уклав договори про надання кваліфікованих електронних довірчих послуг, до іншого кваліфікованого надавача електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 23.07.2024 № 842;
- Таблиці транслітерації українського алфавіту латиницею, затвердженої постанови Кабінету Міністрів України від 27.01.2010 № 55, зі змінами та доповненнями;
- Положення про синхронізацію часу у програмно-технічних комплексах кваліфікованих надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру, затвердженого постановою Правління Національного банку України від 24.12.2019 № 153;

- Положення про здійснення банками фінансового моніторингу, затвердженого постановою Правління Національного банку України від 19.05.2020 № 65, зі змінами та доповненнями;
- Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України від 28.09.2017 № 95;
- Положення про організацію внутрішнього аудиту в банках України, затвердженого Постановою Правління Національного банку України від 10.05.2016 № 311, зі змінами та доповненнями (далі - Положення НБУ № 311);
- інших актів законодавства України у сфері електронних довірчих послуг.

1.2.3. Вимоги цього Регламенту є обов'язковими до виконання працівниками Надавача.
1.2.4. Будь-яка зацікавлена особа може ознайомитися з положеннями цього Регламенту на веб-сайті Надавача.
1.2.5. Ознайомлення з вимогами цього Регламенту та їх визнання Клієнтами перед укладенням Договору про надання електронних довірчих послуг є обов'язковою умовою та підставою для підписання з ними Договору про надання електронних довірчих послуг,
1.2.6. 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.

1.3. Внесення змін та доповнень до цього Регламенту

1.3.1. Внесення змін та доповнень до цього Регламенту здійснюється Надавачем відповідно до вимог законодавства України.
1.3.2. Про внесення змін та доповнень до цього Регламенту, Надавач повідомляє шляхом розміщення зазначених змін та доповнень на веб-сайті Надавача.
1.3.3. Усі зміни та доповнення, внесені до цього Регламенту, що не пов'язані зі зміною законодавства України, набувають чинності через 10 (десять) календарних днів з моменту розміщення зазначених змін і доповнень на веб-сайті Надавача.
1.3.4. Усі зміни та доповнення, внесені Надавачем до цього Регламенту у зв'язку зі зміною законодавства України, набувають чинності за результатом погодження засвідчувальним центром змін та доповнень до Регламенту з моменту публікації погоджених засвідчувальним центром змін до цього Регламенту на веб-сайті Надавача.
1.3.5. Усі зміни та доповнення до цього Регламенту, з моменту їх вступу в дію, однаково поширюються на всіх Клієнтів, що приєдналися до Договору про надання електронних довірчих послуг.
1.3.6. Якщо Клієнт не згоден із внесеними змінами та доповненнями, він має право припинити використання послуг.

2. ЗАГАЛЬНІ ВІДОМОСТІ ПРО НАДАВАЧА

2.1. Повне найменування юридичної особи Надавача: АКЦІОНЕРНЕ ТОВАРИСТВО «УНІВЕРСАЛ БАНК».
2.2. Скорочене найменування юридичної особи: АТ «УНІВЕРСАЛ БАНК».
2.3. Повне найменування Надавача: Кваліфікований надавач електронних довірчих послуг monobank | Universal Bank АТ «УНІВЕРСАЛ БАНК».
2.4. Скорочене найменування Надавача: КНЕДП monobank | Universal Bank АТ «УНІВЕРСАЛ БАНК»
2.5. Код ЄДРПОУ: 21133352.
2.6. Юридична адреса Надавача: 04082, Україна, м. Київ, вул. Автозаводська, 54/19.
2.7. Адреса розміщення головного офісу Надавача: 04071, Україна, м. Київ, вулиця Оленівська, 23.
2.8. У разі перенесення роботи Надавача до віддаленого резервного пункту та/або виникнення критичних ситуацій, інформування про зміну схеми обслуговування Клієнтів буде забезпечено шляхом розміщення відповідної інформації на веб - сайті Надавача.
2.9. Телефонні номери Надавача, телефонні номери його ВПР (за наявності) та адреси його ВПР (за наявності) публікуються на веб-сайті Надавача.
2.10. Електронна адреса веб-сайту Надавача: https://ca.monobank.ua.
2.11. Адреса електронної пошти головного офісу Надавача: ca@universalbank.com.ua .
2.12. Режим роботи Надавача та його ВПР (за наявності) визначається розпорядчими документами Надавача та публікується на веб-сайті Надавача.

2.13. У святкові та передсвяткові дні режим роботи встановлюється розпорядженням НБУ. Про можливі зміни в графіку роботи додатково повідомляється на веб-сайті Надавача.
2.14. Під час повітряних тривог (на період воєнного стану в Україні) обслуговування Клієнтів за адресою Надавача призупиняється.
2.15. Головний офіс Надавача представлений окремим підрозділом Банку, що здійснює надання кваліфікованих електронних довірчих послуг та забезпечує виконання вимог законодавства України до Надавачів.
2.16. Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені Банку.
2.17. Форма Договору про надання кваліфікованих електронних довірчих послу, затверджується Банком та публікується на веб-сайті Надавача.

3. ПЕРЕЛІК ІНФОРМАЦІЇ, ЩО РОЗМІЩУЄТЬСЯ НА ВЕБ-САЙТІ НАДАВАЧА

3.1. Веб-сайт Надавача призначено для розміщення на ньому наступної відкритої інформації:
- відомості про Надавача, режим його роботи та відокремлені пункти реєстрації;
- перелік кваліфікованих електронних довірчих послуг, які надає Надавач;
- перелік та форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;
- цей Регламент або частина цього Регламенту, що стосується взаємодії Надавача з Клієнтами;
- кваліфіковані сертифікати відкритих ключів Надавача;
- кваліфіковані сертифікати відкритих ключів Клієнтів, які надали згоду на їхню публікацію;
- відомості про обмеження під час використання кваліфікованих сертифікатів відкритих ключів;
- інформацію про порядок перевірки чинності сертифіката відкритого ключа;
- перелік нормативно-правових актів у сфері електронної ідентифікації та електронних довірчих послуг;
- реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів (включаючи 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.

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

4. ПЕРЕЛІК КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

4.1. Перелік кваліфікованих електронних довірчих послуг, що надаються Надавачем:
- 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.

4.2. Окрім надання кваліфікованих електронних довірчих послуг, Надавач надає консультаційні послуги за зверненням Клієнтів.
4.3. Надання послуг, зазначених у пунктах 4.1. та 4.2. цього Регламенту, здійснюється Надавачем у відповідності до цього Регламенту та на підставі підписаних Договорів про надання електронних довірчих послуг.

5. ПЕРЕЛІК ПОСАД ТА ФУНКЦІЇ ПРАЦІВНИКІВ НАДАВАЧА

5.1. Працівники Надавача

5.1.1. Надавач для надання довірчих послуг призначає внутрішнім розпорядчим документом працівників, які виконують функції:

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

5.2. Керівник Надавача

5.2.1. Керівник Надавача в межах виконання своїх обов'язків:
- здійснює загальне керівництво діяльністю Надавача і контроль за його діяльністю;
- дає доручення, обов’язкові для працівників Надавача, які виконують функції адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, Аудитора системи, адміністратора безпеки;
- погоджує документи, що визначають організаційні, технічні та технологічні умови діяльності Надавача;
- затверджує інструкції, проектну й експлуатаційну документацію;
- підписує документи, які Надавач подає до засвідчувального центру;
- здійснює представництво та захист інтересів Надавача в сфері кваліфікованих електронних довірчих послуг.

5.2.2. Керівник Надавача зобов’язаний забезпечити створення умов для безперервної особистої освіти та постійне підвищення кваліфікації працівників Надавача у сферах захисту персональних даних, інформаційних технологій, захисту інформації або кібербезпеки.

5.2.3. Керівником Надавача повинна бути встановлена чітка система контролю за дотриманням працівниками Надавача своїх посадових обов’язків, вимог нормативно-правових актів у сфері електронних довірчих послуг і вимог внутрішньої організаційно-розпорядчої документації Надавача та документації щодо СУІБ.

5.3. Заступник керівника Надавача

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

5.4. Адміністратор реєстрації

5.4.1. Адміністратор реєстрації та працівник відокремленого пункту реєстрації, на якого покладено обов’язок з реєстрації Клієнтів, відповідає за:
- ідентифікацію, автентифікацію, верифікацію та реєстрацію Клієнтів;
- надання допомоги Клієнтам під час генерації пар ключів (у разі необхідності);
- опрацювання документів і запитів, наданих Клієнтами;
- перевірка законності звернень про блокування, поновлення та скасування сертифікатів ключів Клієнтів;
- перевірка документів, наданих Клієнтами заяв про формування, блокування, поновлення та скасування сертифікатів ключів;
- надання допомоги Клієнтам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вживання заходів щодо забезпечення безпеки інформації під час генерації;
- надання консультацій щодо умов та порядку надання кваліфікованих електронних довірчих послуг, які надає Надавач;
- встановлення належності відкритого ключа та відповідного йому особистого ключа Клієнту;
- ведення обліку Клієнтів.

5.5. Адміністратор сертифікації

5.5.1. 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.

5.5.2. Основними обов'язками адміністратора сертифікації є:
- участь у генерації пар ключів Надавача та створенні резервних копій особистих ключів Надавача (зазначену у цьому абзаці генерацію здійснює адміністратор сертифікації у присутності та під контролем адміністратора безпеки);
- зберігання особистих ключів Надавача та їх резервних копій;
- забезпечення використання особистих ключів Надавача під час формування та обслуговування сертифікатів ключів Надавача та Клієнтів;
- участь у знищенні особистих ключів Надавача та їх резервних копій (зазначене у цьому абзаці знищення здійснює адміністратор сертифікації у присутності та під контролем адміністратора безпеки);
- забезпечення ведення, архівування та відновлення баз даних сертифікатів ключів Клієнтів;
- забезпечення публікації сертифікатів ключів Клієнтів та СВС на веб-сайті Надавача;
- створення резервних копій сертифікатів ключів Клієнтів;
- зберігання сертифікатів відкритих ключів Клієнтів, їх резервних копій, СВС та інших резервних копій, які передбачені вимогами законодавства України в сфері електронних довірчих послуг.

5.6. Адміністратор безпеки

5.6.1. Адміністратор безпеки відповідає за:
- належне функціонування СУІБ;
- проведення перевірок дотримання адміністраторами реєстрації, адміністраторами сертифікації, Аудиторами системи, системними адміністраторами працівниками ВПР, на яких покладено обов'язки реєстрації Клієнтів, вимог документації щодо СУІБ. Періодичність проведення таких перевірок –не рідше ніж один раз на рік.

5.6.2. Основними обов'язками адміністратора безпеки є:
- здійснення контролю за генерацією пар ключів Надавача та створенні резервних копій особистих ключів Надавача (зазначену у цьому абзаці генерацію здійснює адміністратор сертифікації у присутності та під контролем адміністратора безпеки);
- контроль за формуванням, обслуговуванням і створенням резервних копій сертифікатів ключів Надавача, Клієнтів та СВС;
- контроль за зберіганням особистих ключів Надавача та їх резервних копій, особистих ключів адміністраторів;
- здійснення контролю за знищенням особистих ключів Надавача та їх резервних копій (зазначене у цьому абзаці знищення здійснює адміністратор сертифікації у присутності та під контролем адміністратора безпеки), контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;
- організація розмежування доступу до ресурсів ІКС Надавача;
- контроль за функціонуванням СУІБ;
- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування СУІБ після збоїв, відмов, аварій ІКС Надавача;
- забезпечення режиму доступу до приміщень Надавача, в яких розміщена ІКС Надавача;
- ведення журналів обліку адміністратора безпеки, визначених документацією СУІБ;
- проведення перевірок відповідності положень внутрішньої організаційно-розпорядчої документації Надавача та документації щодо СУІБ;
- контроль за дотриманням працівниками Надавача положень внутрішньої організаційно-розпорядчої документації Надавача та документації щодо СУІБ;
- контроль за веденням реєстру Надавача;
- контроль за веденням архіву Надавача.

5.6.3. Забороняється суміщення обов'язків адміністратора безпеки з обов'язками адміністратора реєстрації, адміністратора сертифікації, аудитора системи, системного адміністратора та працівників ВПР, на яких покладені обов'язки з реєстрації Клієнтів.

5.6.4. Адміністратором безпеки може бути особа, яка має стаж роботи у сфері захисту інформації або кібербезпеки не менше 3 (трьох) років та відповідає хоча б одній з умов:

1) має вищу освіту за спеціальністю у сферах захисту інформації або кібербезпеки;

2) має вищу освіту за спеціальністю у сфері інформаційних технологій та пройшла курси підвищення кваліфікації у сфері захисту інформації або кібербезпеки.

5.7. Аудитор системи

5.7.1. Аудитор системи відповідає за виявлення недоліків у функціонуванні СУІБ та своєчасне інформування про це Керівника Надавача, заступника Керівника Надавача та адміністратора безпеки.

5.7.2. Аудитор системи здійснює перегляд архівів та журналів аудиту подій ІКС Надавача.

5.7.3. Основними обов'язками Аудитора системи є:

- перегляд та у разі виявлення недоліків функціонування СУІБ проведення перевірок цілісності архівів, а також журналів аудиту подій, що реєструють технічні засоби ІКС Надавача;
- забезпечення спостереження за функціонуванням СУІБ (реєстрація подій в ІКС Надавача, моніторинг подій тощо);
- участь у розслідуванні інцидентів з безпеки в ІКС Надавача.

5.8. Системний адміністратор

5.8.1. Системний адміністратор відповідає за належне функціонування засобів та обладнання ІКС Надавача.

5.8.2. Основними обов'язками системного адміністратора є:

- організація експлуатації та технічного обслуговування ІКС Надавача і адміністрування її технічних засобів;
- забезпечення функціонування веб-сайту Надавача;
- участь у впровадженні та забезпеченні функціонування СУІБ в ІКС Надавача;
- забезпечення ведення журналів аудиту подій, що реєструють технічні засоби ІКС Надавача;
- встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального ПЗ ІКС Надавача;
- встановлення та налагодження штатної підсистеми резервного копіювання бази даних ІКС Надавача;
- забезпечення актуалізації баз даних, створюваних та оброблюваних в ІКС Надавача, у зв'язку зі збоями.

6. ПОЛІТИКА СЕРТИФІКАТА

6.1. **Перелік сфер, в яких дозволяється використання кваліфікованих сертифікатів відкритих ключів, сформованих Надавачем**

6.1.1. **Кваліфіковані сертифікати відкритих ключів, сформованих Надавачем, дозволено використовувати для:**

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

6.1.1.1. 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 Розширення сертифіката "Призначення відкритого ключа" ("keyUsage")

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

6.1.1.2. 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.

6.1.1.3. У випадках, передбачених вимогами до окремо визначених ІКС, 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.

6.1.2. **Обмеження щодо використання кваліфікованих сертифікатів відкритих ключів, сформованих Надавачем**

6.1.2.1. Підставою для оброблення персональних даних у кваліфікованих сертифікатах відкритих ключів, сформованих Надавачем є згода суб’єктів персональних даних на оброблення їхніх персональних даних. Така згода оформляється у вигляді письмового дозволу на оброблення персональних даних, у якому задокументовано добровільне волевиявлення фізичних осіб щодо надання дозволу на оброблення їхніх персональних даних.

6.1.2.2. Форма дозволу суб’єктів персональних даних на оброблення їхніх персональних даних у кваліфікованих сертифікатах відкритих ключів, сформованих Надавачем розміщується на веб-сайті Надавача. Дозвіл на оброблення персональних даних надають ті суб’єкти персональних даних, чиї персональні дані вперше передаються до Надавача. Клієнт забезпечує подання до Надавача дозволу на оброблення персональних даних разом із відповідною заявою (запитом) на формування сертифіката.

6.1.2.3. Формування та подання Надавачу запитів для формування кваліфікованих сертифікатів відкритих ключів означає, що Клієнт ознайомлений із вимогами пункту 6.1.2 цього Регламенту та надає згоду на опрацювання Надавачем його персональних даних у кваліфікованих сертифікатах відкритих ключів для цих цілей протягом усього терміну зберігання цих сертифікатів, а також персональних даних, що включені до документованої інформації. Не допускається формування кваліфікованих сертифікатів відкритих ключів без згоди Клієнта для оброблення персональних даних у цих кваліфікованих сертифікатах відкритих ключів.

6.1.2.4. Не допускається використання кваліфікованих сертифікатів відкритих ключів, сформованих Надавачем для певної сфери із відповідним розширенням сертифіката, в інших сферах.

6.1.2.5. Надавач забезпечує чітке та вичерпне повідомлення будь-якій особі, яка звернулася за отриманням електронної довірчої послуги, про умови використання такої послуги, у тому числі про будь-які обмеження її використання, перед укладенням Договору про надання електронних довірчих послуг, шляхом включення відповідної інформації в затверджений Надавачем публічний договір або цей Регламент, що розміщується на веб-сайті Надавача.

6.1.2.6. Про обмеження використання кваліфікованих сертифікатів відкритих ключів сформованих Надавачем з технічних причин Надавач інформує користувачів електронних довірчих послуг шляхом розміщення даної інформації на веб-сайті Надавача.

6.1.2.7. У разі якщо Надавач належним чином заздалегідь повідомить користувачів електронних довірчих послуг про обмеження щодо використання електронних довірчих послуг, які він надає, за умови що такі обмеження є зрозумілими для користувачів, він не несе відповідальності за шкоду, завдану внаслідок використання електронних довірчих послуг з порушенням зазначених обмежень.

6.1.3. **Перелік сертифікатів відкритих ключів Надавача**

6.1.3.1. 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, які використовуються для надання інформації про статус кваліфікованих сертифікатів відкритих ключів Клієнтів за запитом про статус кваліфікованого сертифіката в режимі реального часу;
3) кваліфіковані сертифікати відкритих ключів Надавача, сформовані засвідчувальним центром, що використовуються для формування та перевірки електронних позначок часу.

6.1.4. **Час і порядок публікації кваліфікованих сертифікатів відкритих ключів та списків відкликаних сертифікатів**

6.1.4.1. Надавач публікує на веб-сайті:

- кваліфіковані сертифікати відкритих ключів засвідчуваного центру;
- кваліфіковані сертифікати відкритих ключів Надавача;
- кваліфіковані сертифікати відкритих ключів Клієнтів, які надали згоду на публікацію їхніх сертифікатів (необмежений пошук);
- кваліфіковані сертифікати відкритих ключів інших Клієнтів Надавача (обмежений пошук з використанням особистого ключа, при цьому перегляд на веб-сайті Надавача доступний лише Клієнту власнику сертифіката);
- повний та частковий СВС.

6.1.4.2. **Публікація чинних кваліфікованих сертифікатів відкритих ключів**

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

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

6.1.4.3. **Списки відкликаних сертифікатів**

Надавач формує СВС 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 СВС 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.

6.1.4.4. **Публікація кваліфікованих сертифікатів відкритих Надавача**

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

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

6.1.5. **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.

6.1.6. **Умови ідентифікації та автентифікації Клієнта**

6.1.6.1. **Загальні положення**

Ідентифікація та автентифікація Клієнта Надавачем під час формування та видачі кваліфікованого сертифіката відкритого ключа здійснюється відповідно до вимог статті 22 Закону, пунктів 34-34^3 Положення про КНЕДП.

Обов'язковою умовою надання послуг Клієнтові є перевірка його цивільної правоздатності та дієздатності, а саме юридичної особи (з метою формування кваліфікованого сертифіката електронної печатки або автентифікації веб-сайту) чи фізичної особи - підприємця (з метою формування кваліфікованого сертифіката електронної печатки) Надавач зобов'язаний використовувати інформацію про юридичну особу чи фізичну особу - підприємця, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи, а також пересвідчитися, що обсяг цивільної правоздатності та

дієздатності юридичної особи чи фізичної особи - підприємця є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа або автентифікації веб-сайту.

Перевірка цивільної правоздатності та дієздатності міжнародних організацій, відомості про яких не внесені до Єдиного державного реєстру юридичних осіб, фізичних осіб - підприємців та громадських формувань або торговельного, банківського чи судового реєстру, що ведеться іноземною державою, за місцезнаходженням штаб-квартири міжнародної організації здійснюється з використанням інформації з міжнародного договору або іншого офіційного документа, на підставі якого створена та/або діє міжнародна організація.

Уповноважений представник юридичної особи або фізичної особи - підприємця підписує документи, необхідні для формування та видачі кваліфікованого сертифіката відкритого ключа працівнику юридичної особи або фізичної особи - підприємця. Надавач під час формування та видачі кваліфікованого сертифіката працівнику юридичної особи або фізичної особи - підприємця здійснює ідентифікацію працівника, а також ідентифікацію особи уповноваженого представника юридичної особи або фізичної особи - підприємця відповідно до вимог законодавства України та перевіряє обсяг його повноважень за документом, що визначає повноваження уповноваженого представника юридичної особи або фізичної особи - підприємця, чи з використанням інформації, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи.

Якщо від імені юридичної особи діє колегіальний орган, Надавачу подається документ, у якому визначено повноваження відповідного органу та розподіл обов'язків між його членами.

При процедурі ідентифікації та верифікації Клієнта можуть використовуватися сервіси перевірки чинності документів та ідентифікаційної інформації про особу.

6.1.6.2. **Порядок ідентифікації автентифікації Клієнтів**

Ідентифікація особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката, здійснюється в один із таких способів:

за особистої присутності фізичної особи, фізичної особи - підприємця чи уповноваженого представника юридичної особи - за результатами перевірки відомостей (даних) про особу, отриманими у встановленому законодавством України порядку з Єдиного державного демографічного реєстру, за паспортом громадянина України або іншими документами, виданими відповідно до законодавства України про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи;

віддалено (без особистої присутності особи), з одночасним використанням засобу електронної ідентифікації, що має високий або середній рівень довіри, раніше виданого фізичній особі, фізичній особі - підприємцю чи уповноваженому представнику юридичної особи за особистої присутності, та багатофакторної автентифікації;

за ідентифікаційними даними особи, що містяться у кваліфікованому сертифікаті електронного підпису чи печатки, раніше сформованого (сформованої) та виданого (виданої) згідно з підпунктом 1 або 2 цього пункту, за умови чинності такого сертифіката;

з використанням інших способів ідентифікації, визначених законом, надійність яких є еквівалентною особистій присутності та підтверджена органом з оцінки відповідності.

На період воєнного стану на території України та протягом шести місяців з дня його припинення чи скасування Надавач має право для надання послуги формування кваліфікованого сертифіката здійснювати ідентифікацію та автентифікацію Клієнта, що є фізичною особою чи фізичною особою-підприємцем, відповідно до вимог статті 22 Закону, а також одним із способів визначених п. 34^1 Положення про КНЕДП із врахуванням вимог, визначених пп. 34^2, 34^3 Положення про КНЕДП, а саме:

- Надавач на період воєнного стану на території України та протягом шести місяців з дня його припинення чи скасування має право для надання послуги формування кваліфікованого сертифіката відкритого ключа здійснювати ідентифікацію та автентифікацію Клієнта, що є фізичною особою чи фізичною особою-підприємцем, відповідно до вимог статті 22 Закону, а також одним із таких способів (далі – способи електронної ідентифікації та автентифікації):

1) шляхом здійснення відеоверифікації з дотриманням вимог пунктів 2-10, 13, 14, 16, 17, 20 додатка 3 до Положення про здійснення банками фінансового моніторингу, затвердженого постановою Правління Національного банку України від 19.05.2020 № 65 (зі змінами);

2) із використанням е-паспорта/е-паспорта для виїзду за кордон, кваліфікованого або удосконаленого електронного підпису Клієнта, фотофіксації Клієнта в такому порядку:

Клієнт подає Надавачу з дотриманням вимог Порядку формування та перевірки е-паспорта і е-паспорта для виїзду за кордон, їх електронних копій, затвердженого постановою Кабінету Міністрів України від 18.08.2021 № 911 (зі змінами) (далі - Порядок № 911), електронну копію свого е-паспорта/е-паспорта для виїзду за кордон;

Клієнт подає Надавачу копію свого ідентифікаційного документа (копії сторінок ідентифікаційного документа, що містять ідентифікаційні дані), засвідчену кваліфікованим електронним підписом Клієнта з кваліфікованою електронною позначкою часу або удосконаленим електронним підписом Клієнта, що базується на кваліфікованому сертифікаті відкритого ключа, виданому Надавачем без відомостей про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки (далі - удосконалений електронний підпис, що базується на кваліфікованому сертифікаті Клієнта), з кваліфікованою електронною позначкою часу;

Надавач здійснює фотофіксацію Клієнта та порівнює фотографію Клієнта, що міститься в електронній копії е-паспорта/е-паспорта для виїзду за кордон Клієнта, із фотографією, отриманою Надавачем під час фотофіксації Клієнта;

Надавач порівнює ідентифікаційні дані, що містяться в електронній копії е-паспорта/е-паспорта для виїзду за кордон Клієнта, з ідентифікаційними даними, що містяться в копії ідентифікаційного документа Клієнта та у кваліфікованому електронному підписі Клієнта або удосконаленому електронному підписі, що базується на кваліфікованому сертифікаті Клієнта, на їх відповідність;

3) із використанням засобів національної системи електронної дистанційної ідентифікації Національного банку (далі - Система BankID Національного банку), е-паспорта/е-паспорта для виїзду за кордон, фотофіксації Клієнта в такому порядку:

Клієнт ініціює надання своїх ідентифікаційних даних Надавачу за допомогою Системи BankID Національного банку;

Клієнт подає Надавачу з дотриманням вимог Порядку № 911 електронну копію свого е-паспорта/е-паспорта для виїзду за кордон;

Надавач здійснює фотофіксацію Клієнта та порівнює фотографію Клієнта, що міститься в електронній копії е-паспорта/е-паспорта для виїзду за кордон Клієнта, із фотографією, отриманою Надавачем під час фотофіксації Клієнта;

Надавач порівнює ідентифікаційні дані, отримані за допомогою Системи BankID Національного банку, з ідентифікаційними даними, що містяться в електронній копії е-паспорта/е-паспорта для виїзду за кордон Клієнта, на їх відповідність;

4) із використанням Системи BankID Національного банку, кваліфікованого або удосконаленого електронного підпису Клієнта, фотофіксації Клієнта в такому порядку:

Клієнт ініціює надання своїх ідентифікаційних даних Надавачу за допомогою Системи BankID Національного банку;

Клієнт подає Надавачу копію свого ідентифікаційного документа (копії сторінок ідентифікаційного документа, що містять ідентифікаційні дані), засвідчену кваліфікованим електронним підписом Клієнта з кваліфікованою електронною позначкою часу або удосконаленим електронним підписом, що базується на кваліфікованому сертифікаті Клієнта, з кваліфікованою електронною позначкою часу;

Надавач здійснює фотофіксацію Клієнта в режимі реального часу з використанням алгоритмів, що дають змогу відрізнити реальну людину від репродукції у будь-якому вигляді її зовнішності (наприклад, цифрова репродукція, грим, маска);

Надавач порівнює ідентифікаційні дані, отримані за допомогою Системи BankID Національного банку, з ідентифікаційними даними, що містяться в копії ідентифікаційного документа Клієнта та у кваліфікованому електронному підписі Клієнта або удосконаленому електронному підписі, що базується на кваліфікованому сертифікаті Клієнта, на їх відповідність;

Надавач порівнює фотографію Клієнта, що міститься в копії ідентифікаційного документа, з фотографією, отриманою Надавачем під час фотофіксації Клієнта;

5) із використанням Системи BankID Національного банку, віддаленого кваліфікованого електронного підпису "Дія.Підпис" ("Дія ID"), фотофіксації Клієнта в такому порядку:

Клієнт ініціює надання своїх ідентифікаційних даних Надавачу за допомогою Системи BankID Національного банку;

Клієнт подає копію свого ідентифікаційного документа (копії сторінок ідентифікаційного документа, що містять ідентифікаційні дані), засвідчену з використанням віддаленого кваліфікованого електронного підпису "Дія.Підпис" ("Дія ID") Клієнта;

Надавач здійснює фотофіксацію Клієнта та порівнює фотографію Клієнта, що міститься в копії ідентифікаційного документа, із фотографією, отриманою Надавачем під час фотофіксації Клієнта;

Надавач порівнює ідентифікаційні дані, отримані за допомогою Системи BankID Національного банку, з ідентифікаційними даними, що містяться в копії ідентифікаційного документа Клієнта та в кваліфікованому електронному підписі "Дія.Підпис" ("Дія ID") Клієнта, на їх відповідність.

- Надавач у разі здійснення ідентифікації та автентифікації Клієнта способом, визначеним у підпункті 1 пункту 34[1] Положення про КНЕДП:

1) не може використовувати результати відеоверифікації в разі:

наявності сумнівів щодо чинності (дійсності) ідентифікаційного документа особи, які не спростовані;

наявності ознак того, що на Клієнта (представника Клієнта) чиниться вплив з боку третьої особи;

2) зобов'язаний забезпечити:

документування кожного етапу відеоверифікації;

передавання та зберігання електронних документів, отриманих під час проведення відеоверифікації, у спосіб, що забезпечує неможливість їх модифікації, а також захист таких електронних документів від втрати, знищення, незаконної обробки відповідно до вимог нормативно-правових актів Національного банку з питань забезпечення інформаційної безпеки в банківській системі України;

належну підготовку адміністраторів реєстрації для проведення відеоверифікації перед початком виконання ними обов'язків, пов'язаних зі здійсненням відеоверифікації.

- Надавач у разі здійснення ідентифікації та автентифікації Клієнта одним чи кількома зі способів, визначених у пункті 34[1] Положення про КНЕДП, зобов'язаний:

здійснювати фотофіксацію Клієнта в режимі онлайн таким чином, щоб обличчя особи відображалось анфас, фотозображення було чітким, давало змогу однозначно розпізнати особу Клієнта та не містило зображення іншої особи в кадрі;

формувати Клієнту кваліфікований сертифікат відкритого ключа виключно в разі позитивних результатів перевірок, визначених у підпунктах 2-5 пункту 34[1] Положення про КНЕДП;

забезпечити зберігання отриманої згідно з вимогами пункту 34[1] Положення про КНЕДП інформації протягом строку, встановленого Правилами застосування переліку документів, що утворюються в діяльності Національного банку України та банків України, затвердженими постановою Правління Національного банку України від 27.11.2018 № 130 (зі змінами), для документованої інформації;

протягом шести місяців із дня припинення чи скасування воєнного стану в Україні забезпечити проведення ідентифікації, автентифікації згідно з вимогами статті 22 Закону тих Клієнтів, що були ідентифіковані згідно з пунктом 34[1] Положення про КНЕДП, або скасувати кваліфіковані сертифікати відкритих ключів таких Клієнтів.

Клієнт, що відкрив рахунок у Банку, може ініціювати використання Надавачем раніше отриманих Банком під час відкриття рахунку ідентифікаційних даних Клієнта.

Клієнт, що є уповноваженим представником юридичної особи чи фізичної особи – підприємця, може ініціювати використання Надавачем раніше отриманих Банком під час відкриття рахунку ідентифікаційних даних Клієнта якщо виконано наступні умови:

юридичною чи фізичною особою – підприємцем відкрито рахунок у Банку;

право отримання послуги представником юридичної особи чи фізичної особи – підприємця підтверджено уповноваженим представником цієї юридичної особи чи фізичної особи – підприємця.

Достовірність інформації про уповноваженого представника юридичної особи чи фізичної особи – підприємця встановлюється за інформацією з Єдиного державного реєстру підприємств та організацій України та документів, що підтверджують повноваження уповноваженого представника юридичної особи або фізичної особи - підприємця та опрацьовуються (зберігаються) АТ «УНІВЕРСАЛ БАНК» з моменту відкриття рахунку.

Надавач залишає за собою право підтримувати лише ті способи електронної ідентифікації та автентифікації, які має можливість забезпечити, із одночасним інформуванням користувачів про це на веб-сайті Надавача.

Клієнт перед тим як скористатися способом електронної ідентифікації та автентифікації повинен ознайомитись з вимогами підпункту 6.1.6.2. цього Регламенту та погодитися з вимогами цього пункту цього Регламенту.

6.1.6.3. **Процедура реєстрації Клієнта**

Процедура ідентифікації, автентифікації для реєстрації Клієнта може здійснюватись з використанням способу ідентифікації та автентифікації описаного в пункту 6.1.6.2 цього Регламенту. Реєстрація виконується адміністраторами реєстрації (див. пункт 5.4. цього Регламенту) протягом одного робочого дня після надходження заяви та згідно з режимом роботи Надавача.

При цьому реєстрація Клієнтів у приміщенні Надавача виконується тільки у робочий час в присутності Клієнта на підставі заяви на реєстрацію та формування кваліфікованого сертифіката Клієнта або анкети-заявки про приєднання до «Умов та Правил надання банківських послуг».

Для проведення процедури реєстрації Клієнт або його довірена особа-представник (тільки для юридичних осіб) надають до Надавача такі основні документи та відомості:

1) для юридичних осіб та фізичних осіб - підприємців:

− паспорт (або інші документи, видані відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи) керівника або працівника юридичної особи (фізичної особи – підприємця), та засвідчена у встановленому порядку копія паспорта;

− нотаріально засвідчену копію установчих документів або відповідні відомості з Єдиного державного реєстру підприємств та організацій України;

− документи, що підтверджують повноваження керівника Клієнта;

− копія свідоцтва про реєстрацію платника ПДВ (у разі, якщо особа є платником податку на додану вартість);

− облікова картка платника податків (за наявності) та засвідчена у встановленому порядку копія облікової картки платника податків;

− відомості щодо терміну дії кваліфікованого сертифіката;

− для представників додатково – довіреність встановленої форми, що розміщено на веб-сайті Надавача.

2) для фізичних осіб:

− паспорт (або інші документи, видані відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи) та засвідчена у встановленому порядку копія паспорта;

− облікова картка платника податків (за наявності) та засвідчена у встановленому порядку копія облікової картки платника податків;

− відомості щодо терміну дії кваліфікованого сертифіката.

Парольною фразою являється ключова фраза голосової автентифікації або відповідь на вказане Клієнтом питання.

Отримання юридичними особами та фізичними особами-підприємцями кваліфікованого сертифіката електронної печатки здійснюється в тому ж порядку, що й отримання підписувачами кваліфікованого сертифіката електронного підпису. Для формування кваліфікованого сертифіката електронної печатки до поля заяви, яке містить відомості про обмеження використання кваліфікованого сертифіката, необхідно внести ознаку спеціального (в якості електронної печатки) призначення КЕП.

Адміністратор реєстрації виконує процедуру ідентифікації особи, яка проходить процедуру реєстрації або уповноваженої (довіреної) особи, у відповідності до вимог цього Регламенту та законодавства України.

Після позитивної ідентифікації особи, яка проходить процедуру реєстрації або уповноваженої особи, адміністратор реєстрації приймає документи, виконує встановлену процедуру обліку отриманих документів та передає їх на розгляд адміністратору сертифікації.

У разі відмови у реєстрації, заява на реєстрацію та формування кваліфікованого сертифіката разом з додатками повертається Клієнту з відміткою адміністратора реєстрації про причини відмови у реєстрації.

У разі прийняття позитивного рішення, адміністратор реєстрації після оплати Клієнтом всіх послуг укладає з ним Договір.

Після цього адміністратор реєстрації виконує реєстраційні дії по занесенню реєстраційної інформації до списку (реєстру) Клієнтів Надавача.

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

6.1.6.4. **Ідентифікаційні дані для отримання кваліфікованих електронних довірчих послуг**

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, які вносяться до кваліфікованого сертифіката відкритого ключа 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) чи псевдонім (із зазначенням про використання особою псевдоніма)	Обов'язково	Документальне (паспорт, посвідка на постійне (тимчасове) місце проживання). У разі відсутності в іноземців та осіб без громадянства документів, виданих відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи, їх ідентифікація у спосіб, визначений пунктом 1 частини другої статті 22 Закону, здійснюється за легалізованим належним чином паспортним документом іноземця або документом, що посвідчує особу без громадянства.
РНОКПП	За наявності	Документальне (облікова картка платника податків, паспорт)
Серія (за наявності), номер паспорта громадянина України (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та офіційно повідомили про це відповідний податковий орган і мають відмітку або інформацію в паспорті громадянина України про право здійснювати будь-які платежі за серією та/або номером паспорта)	Обов'язково	Документальне (паспорт громадянина України (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та офіційно повідомили про це відповідний податковий орган і мають відмітку або інформацію в паспорті громадянина України про право здійснювати будь-які платежі за серією та/або номером паспорта))
УНЗР в ЄДДР	За наявності	Документальне (паспорт громадянина України (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та офіційно повідомили про це відповідний податковий орган і мають відмітку або

Ідентифікаційні дані	Обов'язковість надання ідентифікаційних даних	Механізми підтвердження ідентифікаційних даних
		інформацію в паспорті громадянина України про право здійснювати будь-які платежі за серією та/або номером паспорта)))
Номер телефону	Не обов'язково, на вимогу Клієнта про включення до сертифіката	Технічне (відповідно до можливостей ІКС Надавача)
Адреса електронної пошти (за наявності)	Не обов'язково, на вимогу Клієнта про включення до сертифіката	Технічне (відповідно до можливостей ІКС Надавача)
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))

У випадку реєстрації Клієнтів, які мають документи, що підтверджують інформацію про них (ідентифікаційні дані: прізвище, ім'я, по-батькові (за наявності)), що вноситься до сертифіката відкритого ключа, латиницею (з використанням латинського алфавіту), механізм підтвердження інформації про таку особу (для формування кваліфікованих сертифікатів відкритих ключів електронного підпису) здійснюється за цими документами (відомостями з документів, що містять латинські літери).

У випадку необхідності здійснення транслітерації відомостей з наданих Клієнтом документів їх транслітерація відтворюється здійснюється згідно з Таблицею транслітерації українського алфавіту латиницею, затвердженої постановою Кабінету Міністрів України від 27.01.2010 № 55 (із змінами).

Транслітерація прізвищ та імен осіб і географічних назв здійснюється шляхом відтворення кожної літери латиницею.

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 (дані електронних ресурсів ЄДР: https://usr.minjust.gov.ua/content/freesearch та платників ПДВ: https://cabinet.tax.gov.ua/registers/pdv)
Код організації згідно ЄДРПОУ	Обов'язково	Документальне або технічне (дані електронних ресурсів ЄДР: https://usr.minjust.gov.ua/content/freesearch)
Юридична адреса	Не обов'язково	Документальне або технічне (дані електронних ресурсів ЄДР: https://usr.minjust.gov.ua/content/freesearch)
Повноваження або займана посада	На вимогу Клієнта щодо їх включення до сертифікату	Документальне (документи, що ідентифікують посадових осіб,

Ідентифікаційні дані	Обов'язковість надання ідентифікаційних даних	Механізми підтвердження ідентифікаційних даних
		засвідчують право на здійснення діяльності у визначеній сфері: посвідчення, сертифікат, наказ про призначення, свідоцтво тощо) або технічне (дані електронних ресурсів ЄДР: https://usr.minjust.gov.ua/content/freesearch)

Для укладання Договорів про надання кваліфікованих електронних довірчих послуг Надавач може отримувати від Клієнтів інші документи, передбачені законодавством України.

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

6.1.6.5. **Процедура зберігання документів, отриманих від Клієнта, що підтверджують його ідентифікаційні дані**

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 приміщеннях Надавача, архівних сейфах, або архівних шафах Надавача, а також в електронному вигляді із забезпеченням автоматичного резервного копіювання засобами ІКС 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 - Ідентифікаційні дані та механізми їх підтвердження під час встановлення фізичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа

Форма документа	Засвідчення з боку Клієнта		Засвідчення з боку Надавача (адміністратора реєстрації)	
	Тип підпису	Черга засвідчення	Тип підпису	Черга засвідчення
Паперова	Власноручний підпис на паперовому документі	Перша	Власноручний підпис адміністратора реєстрації на паперових документах; КЕП адміністратора реєстрації на електронній копії паперового документу	Друга
Електронна	Удосконалений електронний підпис, що базується на кваліфікованому сертифікаті електронного підпису або кваліфікований електронний підпис	Перша	КЕП адміністратора реєстрації	Друга

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 даних, отриманих в результаті фотофіксації, здійснюється в ІКС Надавача після їх засвідчення шляхом накладання кваліфікованого електронного підпису адміністратора реєстрації.

6.1.7. **Процедура ідентифікації працівників Банку**

6.1.7.1. Якщо до Надавача звертається працівник Банку щодо отримання сертифіката ключа для виконання своїх посадових обов'язків, ідентифікація та верифікація працівника Банку здійснюється за умови його 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. Перелік ідентифікаційних даних та механізми їх підтвердження для формування кваліфікованих сертифікатів відкритих ключів електронного підпису чи печатки наведено у Таблиці 5.

Таблиця 5 - Ідентифікаційні дані та механізми їх підтвердження під час встановлення працівників Банку, 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	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)
Номер телефону	Не обов'язково, на вимогу Клієнта про включення до сертифіката	Технічне (відповідно до можливостей ІКС Надавача)
Адреса банківської електронної пошти	Не обов'язково, на вимогу Клієнта про включення до сертифіката	Технічне (відповідно до можливостей ІКС Надавача)
Займана посада та назва структурного підрозділу	Обов'язково	Документальне (наказ про призначення), або технічне (інформація про облік працівників Банку з інформаційної системи Банку, що містить необхідні дані)

6.1.8. **Механізм автентифікації Клієнтів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований Надавачем**

6.1.8.1. 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.

6.1.8.2. 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.

6.1.8.3. 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.

6.1.8.4. Перевірка ідентифікаційних даних Клієнта, який звертається з заявою в електронній формі, а також законності такого звернення, здійснюється шляхом автентифікації Клієнта за результатами перевірки КЕП або удосконаленого електронного підпису, що базується на кваліфікованому сертифікаті

електронного підпису, на заяві та встановленням на момент подання заяви чинності кваліфікованого сертифіката, що містить ідентифікаційні дані Клієнта. Надавач може здійснити формування кваліфікованого сертифіката за електронною заявою Клієнта, якщо виконані всі нижчезазначені умови:

- кваліфікований сертифікат Клієнта чинний;
- ПЗ, що використовувалось під час генерації пар ключів, є засобом КЕП;
- реєстраційні данні які містяться у чинному кваліфікованому сертифікаті не змінилися;
- особистий ключ відповідний до чинного кваліфікованого сертифіката доступний лише Клієнту та не скомпрометований.

6.1.8.5. Клієнт зобов'язаний у разі зміни своїх ідентифікаційних даних, що містяться у кваліфікованому сертифікаті, сформованому Надавачем, до отримання Клієнтом кваліфікованих електронних довірчих послуг з проведенням його автентифікації за даними такого сертифіката, звернутися до Надавача з повідомленням про настання відповідних змін та надати документи, що їх підтверджують, для скасування чинного кваліфікованого сертифіката та отримання нового.

6.1.8.6. Не допускається використання Клієнтом сертифіката що містить недостовірні ідентифікаційні дані, надані та засвідчені Клієнтом у заяві про формування сертифіката для формування його сертифіката відкритого ключа.

6.1.8.7. Сертифікат блокується та /або скасовується у односторонньому порядку Надавачем у разі отримання ним документального, або технічного (отримання інформації в електронному вигляді з ЄДР, ЄДДР, або ІКС Банку) підтвердження даних про зміну ідентифікаційних даних користувача електронних довірчих послуг, які містяться у сертифікаті відкритого ключа Клієнта, та/або надання користувачем електронних довірчих послуг недостовірних ідентифікаційних даних під час формування його сертифіката відкритого ключа.

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

6.1.9.1. Перелік та опис механізмів ідентифікації, автентифікації, верифікації Клієнтів під час оброблення заяв на блокування, скасування або поновлення кваліфікованого сертифіката ключа наведено у Таблиці 6.

Таблиця 6 - Перелік та опис механізмів ідентифікації, автентифікації, верифікації Клієнтів під час оброблення заяв на блокування, скасування або поновлення кваліфікованого сертифіката ключа

Тип операції (причина подання заяв)	Спосіб подання заяв	Механізми підтвердження ідентифікаційних даних
Блокування кваліфікованого сертифіката відкритого ключа	Усно	За ключовою фразою голосової автентифікації, первинний обмін якою між Клієнтом та Надавачем здійснюється під час подання заяви про формування кваліфікованого сертифіката відкритого ключа
	Письмово на папері	Аналогічні механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа
	Письмово у електронній формі	Аналогічні механізмам підтвердження ідентифікаційних даних Клієнтів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований Надавачем
Скасування кваліфікованого сертифіката відкритого ключа	Письмово на папері	Аналогічні механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого

Тип операції (причина подання заяв)	Спосіб подання заяв	Механізми підтвердження ідентифікаційних даних
		ключа
	Письмово у електронній формі	Аналогічні механізмам підтвердження ідентифікаційних даних к, які мають чинний кваліфікований сертифікат відкритого ключа, сформований Надавачем
Поновлення кваліфікованого сертифіката відкритого ключа	Письмово на папері	методами підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа

6.1.10. **Процедурний контроль**

6.1.10.1. Недотримання 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 СУІБ в межах організації з урахуванням режиму роботи Надавача передбачає дисциплінарні стягнення, адміністративну та кримінальну відповідальність, передбачені:
- Кодексом України про адміністративні правопорушення;
- Кримінальним кодексом України.

6.1.10.2. 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.

6.1.11. **Порядок ведення журналів аудиту подій**

6.1.11.1. Адміністратор реєстрації, адміністратор сертифікації, Аудитор системи, системний адміністратор мають право переглядати журнали аудиту подій в ІКС Надавача, пов'язані з виконанням їх функціональних обов'язків.

6.1.11.2. Надавач забезпечує ведення журналів аудиту подій, в яких реєструються події таких типів:
- спроби створення, знищення, встановлення паролів, зміни прав доступу в ІКС Надавача;
- заміни ПЗ, технічних засобів ІКС Надавача;
- технічне обслуговування ІКС Надавача;
- генерація, використання, знищення особистих ключів Надавача;
- формування, блокування, скасування та поновлення кваліфікованих сертифікатів відкритих ключів, формування СВС;
- спроби несанкціонованого доступу до ІКС Надавача;
- надання доступу адміністраторам до ІКС Надавача;
- збої в роботі ІКС Надавача;
- інші події, що стосуються надання кваліфікованих електронних довірчих послуг.

6.1.11.3. Адміністратор безпеки зобов'язаний вести журнали обліку, передбачені документацією СУІБ.

6.1.11.4. 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.

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

6.1.11.6. Керівник Надавача, заступник керівника Надавача, адміністратор безпеки та Аудитор системи мають право переглядати всі журнали аудиту подій та всі журнали обліку, які ведуться у Надавача.

6.1.11.7. Адміністратор реєстрації, адміністратор сертифікації, системний адміністратор зобов'язані:
- переглядати журнали аудиту подій не рідше 1 (одного) разу на місяць;

- повідомляти адміністратора безпеки про наявність несанкціонованої модифікації в ІКС Надавача, виявлену під час перегляду журналів аудиту подій. Адміністратор безпеки зобов'язаний переглядати журнали аудиту подій не рідше 1 (одного) разу на тиждень.

6.1.11.8. Адміністратор безпеки, Аудитор системи та системний адміністратор під час перегляду журналів аудиту подій вивчають зафіксовані події та перевіряють наявність фактів несанкціонованої модифікації.

6.1.11.9. Після перегляду забезпечується також перевірка наявності та/або перевірка відповідності зберігання наступним вимогам:

6.1.11.10. Резервні копії журналів аудиту подій зберігаються у віддаленому резервному пункті або в Національному центрі резервування державних інформаційних ресурсів із забезпеченням їх захисту від несанкціонованого доступу.

6.1.11.11. Надавач забезпечує зберігання протягом п'яти років з моменту внесення останнього запису:

- журналів аудиту подій;
- журналів обліку, передбачені документацією СУІБ.

6.1.12. **Порядок ведення, збереження, резервування, відновлення, захисту даних, пов'язаних із формуванням та обслуговуванням Надавачем кваліфікованих сертифікатів відкритих ключів**

6.1.12.1. 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 реєстри сформованих кваліфікованих сертифікатів відкритих ключів), СВС протягом строків, встановлених Постановою Правління НБУ «Про затвердження Правил застосування переліку документів, що утворюються в діяльності Національного банку України та банків України» від 27.11.2018 № 130, до передавання на архівне зберігання.

6.1.12.2. Надавач зобов'язаний створити систему резервування та відновлення функціонування ІКС Надавача, яка має забезпечити резервування на основних майданчиках та у віддаленому резервному пункті інформації, із забезпеченням її захисту від несанкціонованого доступу.

6.1.12.3. Види документів та даних, що підлягають зберіганню, строки зберігання, механізм та порядок зберігання і захисту даних наведено у Таблиці 7.

Таблиця 7 - Види документів та даних, що підлягають зберіганню, строки зберігання, механізм та порядок зберігання і захисту даних

Види документів та даних	Форма зберігання	Строк зберігання	Механізм зберігання
Кваліфіковані сертифікати відкритих ключів Надавача	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та/або ручне архівне копіювання на окремі носії інформації
Кваліфіковані сертифікати відкритих ключів Надавача серверів Надавача (OCSP, TSP)	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та/або ручне архівне копіювання на окремі носії інформації
Кваліфіковані сертифікати відкритих ключів адміністраторів Надавача	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та/або ручне архівне копіювання на окремі носії інформації

Види документів та даних	Форма зберігання	Строк зберігання	Механізм зберігання
Кваліфіковані сертифікати відкритих ключів Клієнтів (підписувачів та створювачів електронних печаток)	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та/або ручне архівне копіювання на окремі носії інформації
Журнали аудиту подій ІКС Надавача	Паперова	≥ 5 років	Сховище (сейф)
	Електронна	≥ 5 років	Автоматичне резервне копіювання засобами ІКС Надавача на основних майданчиках та у віддаленому резервному пункті та/або ручне архівне копіювання на окремі носії інформації
Укладені Договори про надання кваліфікованих електронних довірчих послуг	Паперова	Постійно	Архівне приміщення Надавача
	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та/або 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 ІКС Надавача та/або ручне архівне копіювання на окремі носії інформації
	Електронна яка відповідає вимогам пункту 34^1, 34^2 Положення про КНЕДП та відповідно пункту 6.1.6.2 цього Регламенту	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та/або 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 ІКС Надавача та/або ручне архівне копіювання на окремі

Види документів та даних	Форма зберігання	Строк зберігання	Механізм зберігання
			носії інформації
Заяви на блокування кваліфікованих сертифікатів відкритих ключів	Паперова	Постійно	Архівне приміщення Надавача
	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та/або ручне архівне копіювання на окремі носії інформації
Заяви на скасування кваліфікованих сертифікатів відкритих ключів	Паперова	Постійно	Архівне приміщення Надавача
	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та/або ручне архівне копіювання на окремі носії інформації
Заяви на поновлення кваліфікованих сертифікатів відкритих ключів	Паперова	Постійно	Архівне приміщення Надавача
Інша інформація визначена пунктом 2 частини першої статті 25 Закону	Паперова	Постійно	Архівне приміщення Надавача
	Електронна	Постійно	Автоматичне резервне копіювання засобами ІКС Надавача та/або ручне архівне копіювання на окремі носії інформації

6.1.12.4. У разі припинення діяльності Надавача всі документи, на підставі яких Клієнтам надавалися електронні довірчі послуги, кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані сертифікати відкритих ключів - передаються до засвідчувального центру.

6.1.12.5. Для зберігання носіїв з архівними копіями електронних документів виділяється окреме сховище (сейф чи відсік сейфу) з двома примірниками 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.

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

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

6.1.12.8. Відновлення кваліфікованих сертифікатів відкритих ключів з резервної копії здійснюються засобами ІКС Надавача шляхом зчитування кваліфікованих сертифікатів відкритих ключів з останньої (актуальної) резервної копії та запису їх у Реєстр Надавача.

6.1.12.9. Змінні 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.

6.1.12.10. Архівні копії журналів аудиту подій мають зберігатися Надавачем не менше 5-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.

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

6.1.13. **Порядок та умови генерації, зберігання, використання пар ключів кваліфікованого Надавача**

6.1.13.1. 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.

6.1.13.2. 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 04.07.2007 № 243 (зі змінами).

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

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

6.1.13.5. Надавач використовує такі особисті ключі:

- Особистий ключ Надавача;
- Особистий ключ TSP сервера;
- Особистий ключ OCSP сервера;
- Особисті ключі адміністраторів Надавача.

6.1.13.6. Особистий ключ Надавача використовується виключно для формування СВС, кваліфікованих сертифікатів відкритих ключів OCSP сервера, кваліфікованих сертифікатів відкритих ключів Клієнтів.

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

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

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

6.1.13.10. 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.

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

6.1.14. **Порядок та умови резервного копіювання особистого ключа Надавача, збереження, доступу та використання резервних копій**

6.1.14.1. Резервні копії особистих ключів Надавача зберігаються у захищених носіях.

6.1.14.2. 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, які запечатуються або портативні металеві сейфи, які замикаються на ключ та опломбовуються. На конверті/портативному сейфі зазначається дата створення резервних копій, прізвище та ім’я адміністратора сертифікації та номера захищений носіїв з резервними копіями.

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

6.1.14.4. 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 обліку.

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

6.1.15. **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**

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

6.1.15.2. Відкритий та особистий ключі Клієнта можуть бути згенеровані за допомогою засобу КЕП:

- самостійно;
- на робочій станції генерації ключів Клієнтів у Надавача або ВПР;
- самостійно у «хмарному» сховищі ключів Надавача.

6.1.15.3. Унікальність відкритого ключа Клієнта в реєстрі чинних, блокованих та скасованих сертифікатів, унікальність розпізнавального імені Клієнта та унікальність реєстраційного номеру сертифіката в межах Надавача забезпечується адміністратором реєстрації за допомогою засобів ПТК Надавача.

6.1.15.4. У процесі генерації ключових пар Клієнта (для кваліфікованого електронного підпису чи печатки) 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 ПТК Надавача та мають відповідні експертні висновки в сфері КЗІ та ТЗІ.

6.1.15.5. У процесі генерації ключових пар Клієнта (для удосконаленого електронного підпису чи печатки) враховується, що удосконалена електронна печатка відповідає вимогам, встановленим частиною першою статті 171 Закону, а удосконалений електронний підпис, що базується на кваліфікованому сертифікаті електронного підпису, створюється з використанням кваліфікованого сертифіката електронного підпису, виданого Надавачем та не містить відомостей про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису та відповідно Клієнт самостійно визначає спосіб збереження його особистих ключів (може здійснюватись на власних носіях).

6.1.15.6. 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.

6.1.15.7. Після генерації пар ключів Клієнта з використанням апаратно-програмних засобів кваліфікованого та/або удосконаленого електронного підпису чи печатки, які є частиною ПТК Надавача та після формування Надавачем відповідного кваліфікованого сертифіката відкритого ключа, особистий ключ стає доступний Клієнту для використання.

6.1.15.8. Передача запитів для формування кваліфікованих сертифікатів відкритих ключів здійснюється ПЗ ІКС Надавача за участю адміністратора сертифікації, або з використанням самопідписаних запитів для формування кваліфікованих сертифікатів відкритих ключів - автоматично (за умови забезпечення засобами ПЗ ІКС Надавача безперервності процесів генерації пар ключів, формування запитів, передачі їх на обробку захищеними каналами зв'язку, які забезпечують конфіденційність та цілісність даних) по завершенні процедури генерації особистих та відкритих ключів Клієнта.

6.1.15.9. 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.

7. ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

7.1. **Процес подання запиту на формування кваліфікованого сертифіката відкритого ключа**

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

7.1.2. 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.

7.1.3. Обробка запиту на формування кваліфікованого сертифіката відкритого ключа здійснюється ПЗ ІКС 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.

7.1.4. Під час обробки запиту на формування кваліфікованого сертифіката відкритого ключа засобами ІКС 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.

7.1.5. Строк оброблення запиту на формування кваліфікованого сертифіката відкритого ключа, поданого разом із заявою на формування кваліфікованого сертифіката, становить не більше 48 години.

7.2. **Порядок надання сформованого кваліфікованого сертифіката відкритого ключа Клієнту**

7.2.1. 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 веб-сайті Надавача.

7.2.2. 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.

7.2.3. 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.

7.3. **Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа Клієнта на веб-сайті Надавача**

7.3.1. 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.

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

7.4. **Умови використання кваліфікованого сертифіката відкритого ключа Клієнта та його особистого ключа**

7.4.1. Клієнти зобов'язані дотримуватись умов використання особистих ключів та кваліфікованих сертифікатів відкритих ключів в межах зобов'язань, передбачених у статті 12 Закону, 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 про надання кваліфікованих електронних довірчих послуг (між Надавачем та Клієнтом);
- 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.

7.4.2. 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. Див. також вимоги підпунктів 6.1.8.5 та 6.1.8.6. пункту 6. цього Регламенту.

7.4.3. 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.

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

7.5.1. 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.

7.5.2. При цьому, ПЗ ІКС Надавача із інтегрованими засобами кваліфікованого електронного підпису чи печатки, розміщені на 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 чинного 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 ІКС Надавача.

7.5.3. Створення заяви про формування нового кваліфікованого сертифіката відкритого ключа, запиту на формування нового кваліфікованого сертифіката відкритого ключа та їх передача на обробку до ІКС Надавача здійснюється із забезпеченням цілісності та конфіденційності інформації за допомогою засобів кваліфікованого електронного підпису чи печатки.

7.6. **Порядок та умови скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа Клієнта**

7.6.1. 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.

7.6.2. Процедура та перелік підстав для зміни статусу кваліфікованого сертифіката із зазначенням суб'єктів подання запитів на зміну статусу та форм підтвердження підстав наведено у Таблиці 8.

Таблиця 8 - Процедура та перелік підстав для зміни статусу кваліфікованого сертифіката із зазначенням суб'єктів подання запитів на зміну статусу та форм підтвердження підстав

Підстави для зміни статусу сертифіката	Скасування	Блокування	Поновлення	Підтвердження підстав
подання Клієнтом заяви	+	+	+	Заява Клієнта
смерть фізичної особи – підписувача	+			Документальне підтвердження
припинення діяльності створювача електронної печатки	+			Заява Клієнта та/або Документальне або технічне (отримання інформації в електронному вигляді з ЄДР) підтвердження
зміни ідентифікаційних даних Клієнта	+			Заява Клієнта та/або 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 України 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
для працівників Банку - подання заяви про звільнення, вихід у декретну відпустку або у неоплачувану відпустку на період більше 30 днів	+	+		Документальне підтвердження Управління з організаційного розвитку та адміністрування персоналу Департаменту по роботі з персоналом

Підстави для зміни статусу сертифіката	Скасування	Блокування	Поновлення	Підтвердження підстав
для працівників Банку – зміна посади або назви структурного підрозділу	+			Документальне підтвердження Управління з організаційного розвитку та адміністрування персоналу Департаменту по роботі з персоналом

7.6.3. Заява про скасування (блокування, поновлення) кваліфікованого сертифіката електронного підпису чи печатки подається Надавачеві у спосіб, що забезпечує підтвердження особи-Клієнта.

7.6.4. Клієнт має право за власним бажанням здійснити блокування кваліфікованого сертифіката. Під блокуванням кваліфікованого сертифіката розуміється тимчасове призупинення чинності кваліфікованого сертифіката строком до 30 календарних днів.

7.6.5. Після блокування кваліфікованого сертифіката, користувач може протягом 30 календарних днів поновити чинність кваліфікованого сертифіката. Блокований кваліфікований сертифікат буде автоматично скасований Надавачем, якщо протягом зазначеного строку користувач не поновить його чинність.

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

7.6.7. Надавач здійснює цілодобовий прийом заяв Клієнтів в електронній формі про скасування, блокування та поновлення їх кваліфікованих сертифікатів відкритих ключів з використанням інформаційних каналів, відомості про які наведено на веб-сайті Надавача. Усі прийняті у такий спосіб заяви проходять обов'язкову перевірку Надавачем.

7.6.8. Прийом та перевірка заяв у паперовій формі підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів здійснюється Надавачем протягом одного робочого дня після надходження заяви та згідно з режимом роботи Надавача.

7.6.9. 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.

7.6.10. Розірвання Договору про надання довірчих послуг є підставою для скасування Надавачем усіх сертифікатів відкритих ключів, сформованих для Клієнта, якщо таким договором передбачено формування сертифікатів відкритих ключів.

7.7. **Порядок та умови надання інформації про статус кваліфікованих сертифікатів відкритих ключів, сформованих Надавачем**

7.7.1. **Періодичність формування СВС та строки його дії**

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

7.7.1.2. Частковий список відкликаних 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.

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

7.7.2.1. 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 комунікаційні мережі загального користування із використанням протоколу OCSP.

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

7.8. **Строки дії кваліфікованих сертифікатів відкритих ключів, сформованих кваліфікованим Надавачем**

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

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

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

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

7.8.5. 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.

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

8.1. **Надання засобів кваліфікованого електронного підпису чи печатки**

8.1.1. 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.

8.1.2. Надання Надавачем засобів кваліфікованого електронного підпису чи печатки у вигляді апаратно-програмних засобів здійснюється на договірних засадах.

8.1.3. 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 веб-сайт Надавача. Умови надання таких послуг та інша пов’язана з ними інформація публікуються на веб-сайті Надавача.

8.2. **Надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу**

8.2.1. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу надається автоматизовано засобами ПТК Надавача під час створення кваліфікованого або удосконаленого електронного підпису чи печатки та відповідає вимогам, встановленим частиною другою статті 26 Закону.

8.3. **Припинення діяльності Надавача**

8.3.1. Про прийняте рішення про припинення надання кваліфікованих електронних довірчих послуг Надавач повідомляє Клієнтам, засвідчувальному центру, іншому кваліфікованому надавачу (у разі укладення з ним відповідного договору) та контролюючому органу не пізніше п’яти робочих днів з дня прийняття такого рішення.

8.3.2. Припинення діяльності Надавача здійснюється відповідно вимог встановлених статті 31 Закону та у відповідності до погодженого засвідчувальним центром плану припинення діяльності Надавача.

8.3.3. У разі припинення надання кваліфікованих електронних довірчих послуг Надавач зобов’язаний передати засвідчувальному центру, або іншому кваліфікованому надавачу (у разі укладення з ним відповідного договору) 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).

8.4. **Необхідні вимоги до процедур**

8.4.1. 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.

8.4.2. Зазначені вимоги затверджуються як окремий документ Надавача.

9. ІСТОРІЯ ДОКУМЕНТУ

Версія	Дата	Автор (ПІБ, посада)	Опис зміни
1.0.	20.11.2024р.	Карлаш В.В. Начальник відділу кваліфікованого надавача електронних довірчих послуг	Перша версія