ЗАТВЕРДЖУЮ
Голова Правління
АТ “Укрексімбанк”

_____С. О. Єрмаков
“ 14 ” 11 2022 р.

РЕГЛАМЕНТ РОБОТИ НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ АТ “УКРЕКСІМБАНК”

ПОГОДЖЕНО

В.о. начальника управління
інформаційної безпеки

_____П. А. Коломієць
“ 13 ” 10 2022 р.

2022

ЗМІСТ

ВСТУП

Даний регламент є документом надавача електронних довірчих послуг АТ "Укрексімбанк" (далі – НЕДП), який визначає організаційно-методологічні, технічні та технологічні умови діяльності НЕДП, під час надання ним електронних довірчих послуг (далі – Регламент).
Регламент розроблено відповідно до чинного законодавства України у сфері електронних довірчих послуг.
Вимоги Регламенту є обов'язковими для виконання персоналом НЕДП та клієнтами НЕДП.
Суб'єктами правових відносин у сфері електронних довірчих послуг, що обумовлюються цим Регламентом є НЕДП і підисувачі.
Будь-яка зацікавлена особа може ознайомитися з положеннями Регламенту на Веб-порталі (електронному інформаційному ресурсі) НЕДП, в офісах НЕДП та його відокремлених пунктах реєстрації.

ТЕРМІНИ ТА ВИЗНАЧЕННЯ

НЕДП	– Надавач електронних довірчих послуг;
БД	– база даних НЕДП, у якій зберігаються реєстр НЕДП, інформаційно-довідкова, технологічна та інша службова інформація, потрібна для функціонування програмно-технічного комплексу (далі – ПТК) НЕДП;
Відокремлений пункт реєстрації (ВПР)	– представництво (філія, підрозділ, територіальний орган) НЕДП, що здійснює реєстрацію підписувачів з дотриманням вимог чинного законодавства про електронні довірчі послуги;
Відповідальна особа НЕДП	– керівник НЕДП, заступник керівника НЕДП або адміністратори (оператори) НЕДП, визначені у пункті 4 даного Регламенту;
Договір, відповідно до якого підписувачу надаються електронні довірчі послуги	– окремий договір між підписувачем, який є клієнтом АТ "Укрексімбанк" (далі – Банк), та Банком про надання електронних довірчих послуг або договір про обслуговування клієнта Банку, що має містити положення про надання електронних довірчих послуг підписувачу. Підписувачі, які є працівниками Банку, не укладають з НЕДП договір про надання електронних довірчих послуг;
Заявник	– уповноважений представник підписувача, який є клієнтом Банку, який на законних підставах звертається до НЕДП з метою організації та проведення реєстрації підписувача – клієнта Банку, отримання послуг від НЕДП, а також зміни його даних (реквізитів) в установленому порядку;
Зміна ідентифікаційних даних підписувача	– зміна даних підписувача, що внесені до сертифіката підписувача, які попередньо надавалися заявником до НЕДП;
Зміна статусу сертифіката ключа	– виконання однієї з процедур блокування/ скасування/ поновлення сертифіката;

Веб-портал НЕДП	– електронний інформаційний ресурс НЕДП (веб-сайт) – загальнодоступна частина БД. Доступ до інформаційного ресурсу НЕДП є вільним і забезпечується через телекомунікаційні мережі загального користування;
Підписувач	– клієнт банку, якому НЕДП надає електронні довірчі послуги (далі – клієнт Банку), або працівник Банку, який для виконання своїх службових обов'язків користується електронними довірчими послугами НЕДП;
Реєстр НЕДП	– електронна база даних, яка ведеться НЕДП та містить відомості про підписувачів, а також дані, необхідні для надання електронних довірчих послуг.

Інші терміни в цьому Регламенті застосовуються в значеннях, наведених у Законі України "Про електронні довірчі послуги" та нормативно-правових актів Національного банку України з питань застосування електронного підпису.

ПОЗНАЧКИ ТА СКОРОЧЕННЯ

ВПР	- відокремлений пункт реєстрації;
ПТК	- програмно-технічний комплекс;
СВС	- список відкликаних сертифікатів;
ЦОД	- центр обробки даних;
НЕДП	- надавач електронних довірчих послуг;
OCSP	- протокол визначення статусу сертифіката ключа (Online Certificate Status Protocol);
TSP	- протокол фіксування часу;
NTP	- протокол мережевого часу;
НКІ	- носій ключової інформації (USB-токен, HSM, програмний засіб);
ПЗ	- програмне забезпечення;
СУІБ	- система управління інформаційною безпекою;
ЕП	- електронний підпис.

ПОРЯДОК ВНЕСЕННЯ ЗМІН ТА ДОПОВНЕНЬ ДО РЕГЛАМЕНТУ

Внесення змін та доповнень до Регламенту здійснюється НЕДП у відповідності до чинного законодавства України.

Зміни до цього Регламенту можуть бути проведені внаслідок зміни законодавства України у сфері електронних довірчих послуг, розвитку відповідних інформаційних технологій, появи нових міжнародних і національних стандартів України, виправлення помилок тощо.

Про внесення змін та доповнень до цього Регламенту, НЕДП повідомляє шляхом розміщення зазначених змін та доповнень на веб-порталі НЕДП.

1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО НЕДП

1.1. Ідентифікаційні дані НЕДП

Повне найменування Банку:	Акціонерне товариство «Державний експортно-імпортний банк України»
Код ЄДРПОУ Банку:	00032112
Повне найменування НЕДП:	Надавач електронних довірчих послуг АТ «УКРЕКСІМБАНК»
Місцезнаходження НЕДП:	Україна, 03150, м. Київ, вул. Антоновича, 127
Тел./факс:	+380 (44) 247-80-82
Електронна поштова скринька НЕДП:	ca@eximb.com
Електронна адреса веб-порталу НЕДП:	https://ca.eximb.com

2. ПЕРЕЛІК ІНФОРМАЦІЇ, ЩО РОЗМІЩУЄТЬСЯ НЕДП НА ВЕБ-ПОРТАЛІ НЕДП

Веб-портал НЕДП призначено для розміщення на ньому відкритої інформації.
На веб-порталі НЕДП розміщується наступна інформація:

- відомості про НЕДП;
- сертифікати ключів НЕДП;
- перелік електронних довірчих послуг, які надає НЕДП;
- дані про засоби електронного підпису чи печатки, які НЕДП надає клієнтам Банку (у разі коли електрона довірча послуга передбачає використання засобу електронного підпису чи печатки);
- реєстр чинних, блокованих та скасованих сертифікатів ключів;
- відомості про обмеження під час використання сертифікатів ключів, сформованих НЕДП;
- положення чинного регламенту роботи НЕДП;
- нормативно-правові акти України у сфері електронних довірчих послуг;
- довідково-методичні матеріали щодо порядку використання електронних довірчих послуг.

Веб-портал НЕДП доступний цілодобово.

3. ПЕРЕЛІК ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, НАДАННЯ ЯКИХ ЗАБЕЗПЕЧУЄ НЕДП

НЕДП забезпечує надання таких електронних довірчих послуг:

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

4. ОПИС ФУНКЦІЙ АДМІНІСТРАТОРА (ОПЕРАТОРА) РЕЄСТРАЦІЇ, АДМІНІСТРАТОРА СЕРТИФІКАЦІЇ, СИСТЕМНОГО АДМІНІСТРАТОРА, АДМІНІСТРАТОРА БЕЗПЕКИ

Організаційна структура НЕДП містить дві основні складові частини, що виконують адміністративні функції, технічні і технологічні функції.
До адміністративних функцій НЕДП належать:
- реєстрація підписувачів;
- надання підписувачам консультацій з питань, пов'язаних з використанням ЕП;
- розгляд заяв і скарг підписувачів.

До технічних і технологічних функцій ЦСК належать:
- створення і забезпечення функціонування ПТК НЕДП;
- забезпечення захисту інформації впродовж експлуатації ПТК НЕДП;
- генерування і зберігання ключів НЕДП та відповідальних осіб НЕДП;
- надання методологічно-консультативної допомоги під час генерування ключів підписувачів у разі потреби та вживання заходів щодо забезпечення безпеки інформації під час генерування ключів;
- установлення належності підписувачу особистого ключа та його відповідність відкритому ключу;
- формування сертифікатів ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб НЕДП і підписувачів;
- ведення реєстру НЕДП;
- поширення сертифікатів ключів НЕДП і підписувачів у встановленому цим Регламентом порядку;
- блокування, скасування та поновлення сертифікатів ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб НЕДП і підписувачів у випадках, передбачених цим Регламентом і законодавством України у сфері електронних довірчих послуг;
- надання підписувачам послуг фіксування часу;
- надання послуг визначення статусу сертифіката ключа;
- публікація на Веб-порталі НЕДП відкритої інформації;
- інші дії, пов'язані з технічною та технологічною підтримкою діяльності НЕДП.

4.1. Працівники НЕДП

НЕДП для надання довірчих послуг призначає розпорядчим актом працівників, які виконують функції:
- керівника надавача;
- заступника керівника надавача;

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

Керівник надавача та заступник керівника надавача здійснюють загальне керівництво діяльністю надавача і контроль за його діяльністю.

Керівник надавача зобов'язаний забезпечити створення умов для безперервної особистої освіти та постійного підвищення кваліфікації працівників НЕДП у сферах захисту персональних даних, інформаційних технологій, захисту інформації або кібербезпеки. Заступник керівника надавача виконує функції керівника надавача в разі його відсутності або за його письмовим дорученням.

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

- має вищу освіту за спеціальністю у сферах захисту інформації або кібербезпеки;
- має вищу освіту за спеціальністю у сфері інформаційних технологій та пройшла курси підвищення кваліфікації у сфері захисту інформації або кібербезпеки.

Забороняється суміщення обов'язків адміністратора безпеки з обов'язками адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, працівників ВПР, на яких покладено обов'язки з реєстрації клієнтів.

4.2. Керівник НЕДП, заступник керівника

Функції та обов'язки керівника НЕДП:

- дає доручення, обов'язкові для працівників НЕДП, які виконують функції адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, адміністратора безпеки;
- погоджує розпорядчі акти, документи, що визначають організаційні, технічні та технологічні умови діяльності НЕДП;
- затверджує, інструкції, проектну й експлуатаційну документацію;
- затверджує акти введення в експлуатацію оновлень ПТК НЕДП;
- координує дії персоналу НЕДП.

Функції та обов'язки заступника керівника НЕДП:

- дає доручення, обов'язкові для працівників НЕДП, які виконують функції адміністратора реєстрації, адміністратора сертифікації, системного адміністратора, адміністратора безпеки;
- погоджує розпорядчі акти, документи, що визначають організаційні, технічні та технологічні умови діяльності НЕДП;
- затверджує, інструкції, проектну й експлуатаційну документацію;

- координує дії персоналу НЕДП;
- взаємодіє з відповідними підрозділами Банку з питань надання електронних довірчих послуг клієнтам та партнерам Банку;
- організує використання засобів електронного підпису чи печатки у діяльності Банку;
- взаємодіє з розробником ПТК НЕДП;
- планує роботи НЕДП та ведення звітності;
- бере участь в генерації особистих ключів та ключів серверів НЕДП;
- здійснює контроль за виконанням посадовими особами НЕДП вимог цього Регламенту та інших нормативних документів, що регламентують діяльність НЕДП.

4.3. Адміністратор, оператор реєстрації

Адміністратор реєстрації відповідає за:
- ідентифікацію, автентифікацію, верифікацію клієнтів Банку;
- надання допомоги підписувачам під час генерації пар ключів (у разі необхідності);
- опрацювання документів і запитів, наданих клієнтами.

Оператори реєстрації виконують обов'язки з реєстрації клієнтів Банку у ВПР.
Основними обов'язками адміністратора реєстрації є:
- ідентифікація та автентифікація, реєстрація підписувачів;
- перевірка законності звернень про блокування, поновлення та скасування сертифікатів ключів підписувачів;
- перевірка документів, наданих клієнтами заяв про формування, блокування, поновлення та скасування сертифікатів ключів;
- надання допомоги підписувачів 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 електронних довірчих послуг НЕДП;
- встановлення належності відкритого ключа та відповідного йому особистого ключа підписувачу;
- ведення обліку підписувачів.

4.4. Адміністратор сертифікації

Адміністратор сертифікації відповідає за:
- формування сертифікатів ключів;
- ведення реєстру чинних, блокованих та скасованих сертифікатів ключів;
- генерацію, створення резервних копій, використання особистих ключів

НЕДП;
- зберігання особистих ключів і резервних копій особистих ключів НЕДП.

Основними обов'язками адміністратора сертифікації є:
- участь у генерації пар ключів НЕДП та створенні резервних копій особистих ключів НЕДП;
- зберігання особистих ключів НЕДП та їх резервних копій;
- забезпечення використання особистих ключів НЕДП під час формування та обслуговування сертифікатів ключів НЕДП та підписувачів;
- участь у знищенні особистих ключів НЕДП та їх резервних копій;
- забезпечення ведення, архівування та відновлення баз даних сертифікатів ключів підписувачів;
- забезпечення публікації сертифікатів ключів підписувачів та СВС на веб-сайті НЕДП;
- створення резервних копій сертифікатів ключів підписувачів;
- зберігання сертифікатів відкритих ключів підписувачів, їх резервних копій, СВС та інших резервних копій, які передбачені СУІБ.

4.5. Системний адміністратор

Системний адміністратор відповідає за належне функціонування ПТК НЕДП.

Основними обов'язками системного адміністратора є:
- організація експлуатації та технічного обслуговування ПТК НЕДП і адміністрування технічних засобів ПТК НЕДП;
- забезпечення функціонування веб-сайту НЕДП;
- участь у впровадженні та забезпеченні функціонування СУІБ;
- ведення журналів аудиту подій, що реєструють технічні засоби ПТК НЕДП;
- встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення ПТК НЕДП;
- встановлення та налагодження штатної підсистеми резервного копіювання бази даних ПТК НЕДП;
- забезпечення актуалізації баз даних, створюваних та оброблюваних в ПТК НЕДП, у випадку збоїв.

4.6. Адміністратор безпеки

Адміністратор безпеки відповідає за:
- належне функціонування СУІБ;
- проведення перевірок дотримання адміністраторами (операторами) реєстрації, адміністраторами сертифікації, системними адміністраторами положень внутрішньої організаційно-розпорядчої документації НЕДП та

документації щодо СУІБ. Періодичність проведення таких перевірок – один раз на рік.

Основними обов'язками адміністратора безпеки є:

- участь у генерації пар ключів НЕДП та створенні резервних копій особистих ключів НЕДП;
- контроль за формуванням, обслуговуванням і створенням резервних копій сертифікатів ключів НЕДП, клієнтів та СВС;
- контроль за зберіганням особистих ключів НЕДП та їх резервних копій, особистих ключів адміністраторів;
- участь у знищенні особистих ключів НЕДП та їх резервних копій, контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;
- організація розмежування доступу до ресурсів ПТК НЕДП;
- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування системи захисту інформації після збоїв, відмов, аварій ПТК НЕДП;
- забезпечення режиму доступу до приміщень НЕДП, в яких розміщено ПТК НЕДП;
- ведення журналів обліку адміністратора безпеки, визначених документацією щодо СУІБ;
- проведення перевірок журналів аудиту подій, що реєструють технічні засоби ПТК НЕДП;
- контроль за дотриманням працівниками НЕДП положень внутрішньої організаційно-розпорядчої документації НЕДП;
- контроль за веденням реєстру НЕДП;
- контроль за веденням архіву НЕДП.

5. ПОЛІТИКА СЕРТИФІКАТА

5.1. Перелік сфер, в яких дозволяється використання сертифікатів ключів, сформованих НЕДП

Сертифікати ключів, які формуються НЕДП, призначені для забезпечення діяльності фізичних та юридичних осіб (фізичних осіб – підприємців), яка здійснюється з використанням електронних документів.

Електронний підпис, який перевіряється з використанням сертифікатів ключів, що формуються НЕДП, використовується фізичними та юридичними особами (фізичними особами – підприємцями) – суб'єктами електронного документообігу – для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Перелік сфер, у яких дозволяється використання сертифікатів:

- перевірка електронного підпису чи печатки;
- автентифікація;
- узгодження ключів шифрування.

Управління особистими ключами клієнтів Банку у засобах електронного підпису клієнтів включає:

- генерацію особистих ключів на засобах електронного підпису та формування запитів на формування сертифікатів ключів;
- можливість зміни паролю доступу до особистих ключів на засобах електронного підпису;
- можливість знищення особистих ключів на засобах електронного підпису;
- шифрування та розшифрування даних;
- створення електронного підпису.

У таблиці 1 наведені значення, які НЕДП встановлює під час формування сертифіката ключа у розширенні "Призначення відкритого ключа" ("keyUsage") для ідентифікації сфери використання сертифікатів ключів.

Таблиця 1

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

5.2. Обмеження щодо використання сертифікатів ключів, сформованих НЕДП

Обмеження щодо використання сформованих НЕДП сертифікатів ключів застосовуються у відповідності до положень цього Регламенту та діючого законодавства України у сфері електронних довірчих послуг.
НЕДП має право встановлювати обмеження сфери використання сформованих ним сертифікатів ключів. Інформація щодо обмеження сфери використання сертифікату ключа зазначається у сформованому сертифікаті ключа у вигляді уточненого призначення ключа.
Не допускається використання сертифікатів ключів, сформованих НЕДП для певної сфери із відповідним розширенням сертифіката ключа, в інших сферах.

5.3. Час і порядок публікації сертифікатів ключів та списків відкликаних сертифікатів

Інформація щодо формування сертифікатів ключів підписувачів та самі сертифікати ключів розміщуються на Веб-порталі НЕДП безпосередньо після їх формування.
Публікація списків відкликаних сертифікатів здійснюється на Веб-порталі НЕДП автоматично, одразу після їх формування.
НЕДП виконує формування списків відкликаних сертифікатів двох типів:
- повний список;
- частковий список.

Повний список формується один раз на тиждень та містить інформацію про всі сертифікати, сформовані в НЕДП за допомогою власного особистого ключа НЕДП, статус яких був змінений.
Частковий список формується та поширюється кожні 2 години та містить інформацію про всі сертифікати, статус яких був змінений у межах часу випуску останнього повного СВС та часу формування поточного часткового СВС.
Новий СВС може бути опублікований до визначеного часу видання наступного списку, вказаного у поточному списку відкликаних сертифікатів.
Посилання на повний СВС та частковий СВС вносяться до сертифікатів ключів, сформованих НЕДП. У кожному СВС зазначається дата й час формування поточного СВС та дата й час формування наступного СВС.

5.4. Механізм підтвердження володіння особистим ключем, відповідний якому відкритий ключ надається для формування сертифіката ключа

Для формування сертифікатів ключів використовуються запити на формування сертифікатів ключів підпису та шифрування, які створюються в процесі генерації особистого та відкритого ключів.
Відкритий ключ підписувача подається для формування сертифіката ключа виключно у вигляді самопідписаного відповідним йому особистим ключем запиту. Також НЕДП підтримується механізм використання «стартових» ключів. Належність підписувачу особистого ключа, що відповідає відкритому ключу, наданому для формування сертифіката ключа, підтверджується шляхом перевірки в НЕДП удосконаленого електронного підпису на запиті на формування сертифіката ключа.
Підтвердження володіння підписувачем особистим ключем здійснюється без розкриття особистого ключа.

5.5. Умови ідентифікації, автентифікації та верифікації клієнта НЕДП[1]

Формування та видача сертифіката ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у сертифікаті ключа, не допускається.

При процедурі встановлення особи-заявника використовуються сервіси перевірки чинності документів та ідентифікаційної інформації про особу, зокрема:
- «Перевірка за базою недійсних документів» (nd.dmsu.gov.ua);
- «Єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань» (usr.minjust.gov.ua).

Заява для отримання сертифіката ключа підписувачем може мати електронний вигляд, у такому випадку вона повинна бути підписана кваліфікованим електронним підписом (КЕП) клієнта та надана адміністратору реєстрації НЕДП електронною поштою або на носії інформації. Заява, яка має електронний вигляд, приймається до розгляду лише у разі позитивної перевірки КЕП та ідентифікації особи клієнта. При процедурі встановлення підтвердження цілісності електронних документів адміністратором реєстрації НЕДП, використовуються засоби кваліфікованого електронного підпису.

[1] документи, які клієнт Банку повинен надати для отримання електронних довірчих послуг, вимоги щодо особистої присутності клієнта Банку

5.5.1. Фізична особа

Ідентифікація фізичної особи, яка звернулася за отриманням електронної довірчої послуги формування, перевірки та підтвердження чинності сертифіката електронного підпису чи печатки, здійснюється виключно за умови її особистої присутності за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.
Допускається ідентифікація фізичної особи за ідентифікаційними даними, що містяться у раніше сформованому НЕДП сертифікаті ключа, за умови чинності цього сертифіката.
При ідентифікації фізичної особи з'ясовують:
- прізвище, ім'я та по-батькові;
- реєстраційний номер облікової картки платника податків;
- серія та номер паспорта громадянина України або номер паспорта виготовленого у формі картки, що містить безконтактний електронний носій (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта);
- унікальний номер запису в Єдиному державному демографічному реєстрі (за наявності).

5.5.2. Іноземці

Ідентифікація іноземців здійснюється відповідно до законодавства, зокрема, посвідки на проживання особи, яка мешкає в Україні, а також національного паспорта іноземця, або документа, що його замінює.

5.5.3. Юридична особа та представник юридичної особи

Встановлення юридичної особи здійснюється за установчими документами юридичної особи або копіями таких документів, які нотаріально засвідчені, або за даними з Єдиного державного реєстру підприємств та організацій України:
- повне та скорочене найменування організації;
- місцезнаходження організації;
- документи, що ідентифікують посадових осіб, які звернулися за отриманням сертифікатів ключів та визначають їх повноваження;
- код організації згідно Єдиного державного реєстру підприємств та

організацій України.
Під час перевірки цивільної правоздатності та дієздатності юридичної особи НЕДП зобов'язаний ознайомитися з інформацією про юридичну особу, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань, а також пересвідчитися, що обсяг її цивільної правоздатності та дієздатності є достатнім для формування та видачі сертифіката ключа.
НЕДП під час формування та видачі сертифіката ключа здійснює ідентифікацію особи уповноваженого представника юридичної особи відповідно до вимог цього Регламенту, а також перевіряє обсяг його повноважень за документом або за даними з Єдиного державного реєстру юридичних осіб, фізичних осіб - підприємців та громадських формувань, що визначають повноваження представника.
Якщо від імені юридичної особи діє колегіальний орган, до НЕДП подається документ, у якому визначено повноваження відповідного органу та розподіл обов'язків між його членами.

5.5.4. Співробітник Банку

При ідентифікації співробітника з'ясовують:
- табельний номер співробітника Банку;
- прізвище, ім'я та по-батькові;
- реєстраційний номер облікової картки платника податків;
- серію та номер паспорта громадянина України або номер паспорта виготовленого у формі картки, що містить безконтактний електронний носій (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган та мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта);
- унікальний номер запису в Єдиному державному демографічному реєстрі (за наявності).

НЕДП формує сертифікат ключа працівнику Банку тільки після здійснення його ідентифікації й автентифікації з використанням інформаційно-телекомунікаційних систем Банку, що містять необхідні дані. Або за умови особистої присутності працівника за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів, щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

5.6. Механізм автентифікації підписувачів, які мають чинний сертифікат ключа, сформований НЕДП

В НЕДП існують наступні механізми автентифікації для підписувачів, які мають чинний сертифікат ключа, сформований в НЕДП:

- при особистому зверненні: паспорт або інший документ, який посвідчує особу підписувача (для фізичної особи, фізичної особи-підприємця); паспорт, який посвідчує особу представника і наказ про призначення особи на посаду (для представника юридичної особи);
- при зверненні телефонною мережею загального користування: за парольною фразою голосової автентифікації, що вказується підписувачем (заявником) під час реєстрації;
- при зверненні загальнодоступними телекомунікаційними мережами з використанням електронних запитів: електронний підпис, сформований з використанням особистого ключа підписувача.

5.7. Механізм ідентифікації, автентифікації, верифікації підписувачів під час обробки заяв на блокування, скасування або поновлення сертифіката ключа

В залежності від порядку звернення щодо блокування, скасування та поновлення сертифікату ключа передбачені різні форми автентифікації підписувача та перевірки правочинності такого звернення:

- при письмовому (паперовому) зверненні: лист за підписом підписувача (для фізичної особи, фізичної особи-підприємця); лист на фірмовому бланку за підписом уповноваженої особи заявника, до якого належить підписувач, з проставлянням печатки (для юридичної особи, у разі її наявності);
- у разі звернення підписувача у електронній формі: за електронним підписом, створеним за допомогою особистого ключа підписувача (у разі чинності відповідного сертифіката ключа підписувача) та електронної печатки організації заявника (для юридичних осіб та фізичних осіб – підприємців, у разі її наявності);
- у разі звернення щодо блокування сертифікату ключа телефонною мережею загального користування: за парольною фразою голосової автентифікації, що вказується підписувачем (заявником) під час реєстрації.

Підписувач має право подати до НДЕП заяви про блокування, скасування або поновлення сертифіката ключа відповідно до таблиці 2.

Таблиця 2

Назва заяви	Форма заяви
заява про блокування	у формі паперового документа
	у формі електронного документа

	у формі електронного документа з використанням діючого ключа КЕП
	усна форма, по телефону, вказаному на Веб-потралі НЕДП
заява про поновлення	у формі паперового документа
	у формі електронного документа з використанням діючого ключа КЕП
заява про скасування	у формі паперового документа
	у формі електронного документа
	у формі електронного документа з використанням діючого ключа КЕП

5.8. Процедурний контроль[2]

Керівник НЕДП, заступник керівника НЕДП, адміністратор реєстрації, оператор реєстрації, адміністратор сертифікації, системний адміністратор, адміністратор безпеки несуть відповідальність за неналежне виконання своїх обов'язків та розголошення інформації з обмеженим доступом згідно із законодавством України та нормативними документами Банку.

Працівники, які виконують функції, безпосередньо пов'язані із наданням електронних довірчих послуг, приступають до виконання таких функцій після ознайомлення із посадовими інструкціями і попередженнями про відповідальність під особистий підпис.

5.9. Порядок ведення журналів аудиту подій

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

- спроби створення, знищення, встановлення паролів, зміни прав доступу в ПТК НЕДП;
- генерація, використання, знищення особистих ключів НЕДП;
- формування, блокування, скасування та поновлення сертифікатів ключів, формування СВС;
- спроби несанкціонованого доступу до ПТК НЕДП;
- надання доступу адміністраторам до ПТК НЕДП;
- помилки в роботі ПТК НЕДП.

Адміністратор безпеки НЕДП зобов'язаний вести журнали обліку, передбачені

[2] система дисциплінарних стягнень за недотримання відповідальними особами НЕДП своїх обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації НЕДП та документації на СУІБ в межах організації з урахуванням режиму роботи НЕДП

документацією на систему захисту інформації ПТК НЕДП.
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.
НЕДП забезпечує захист журналів аудиту подій від неавторизованого перегляду, несанкціонованої модифікації та від знищення.
Адміністратор реєстрації, адміністратор сертифікації, системний адміністратор мають право переглядати журнали аудиту подій, пов'язані з виконанням їх функціональних обов'язків.
Керівник НЕДП, заступник керівника НЕДП, адміністратор безпеки мають право переглядати всі журнали аудиту подій, які ведуться у НЕДП, та всі журнали обліку, передбачені документацією на систему захисту інформації ПТК НЕДП.
Адміністратор реєстрації, адміністратор сертифікації, системний адміністратор зобов'язані:

- переглядати журнали аудиту подій не рідше одного разу на місяць;
- повідомляти адміністратора безпеки про наявність несанкціонованої модифікації в ПТК НЕДП, виявлену під час перегляду журналів аудиту подій.

Адміністратор безпеки зобов'язаний переглядати журнали аудиту подій не рідше одного разу на тиждень.
НЕДП забезпечує зберігання протягом п'яти років:

- журналів аудиту подій;
- журналів обліку, передбачених документацією на систему захисту інформації ПТК НЕДП.

5.10. Порядок ведення, збереження (із зазначенням строків зберігання), резервування, відновлення, захисту даних, пов'язаних із формуванням та обслуговуванням НЕДП сертифікатів ключів

НЕДП забезпечує зберігання документів, на підставі яких клієнтам надавалися електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані сертифікати ключів, усі сформовані сертифікатів ключів, а також СВС протягом строків, встановлених Правилами застосування переліку документів, що утворюються в діяльності Національного банку України та банків України, затвердженими постановою Правління Національного банку України від 27 листопада 2018 року № 130 (зі змінами), до передавання на архівне зберігання.
НЕДП зобов'язаний створити систему резервування та відновлення функціонування ПТК НЕДП, яка має забезпечити резервування інформації на

основному майданчику та у віддаленому резервному пункті, із забезпеченням її захисту від несанкціонованого доступу.

5.11. Порядок та умови генерації, зберігання, використання пар ключів НЕДП

Власні особисті ключі НЕДП використовуються для формування СВС, сертифікатів ключів послуги OCSP, відповідальних осіб НЕДП та підписувачів.
Особисті ключі НЕДП послуги TSP використовуються під час формування відповіді на запит на позначку часу.
Особисті ключі НЕДП послуги OCSP використовуються під час формування відповіді на запит про статус сертифіката.
Особисті ключі відповідальних осіб НЕДП використовуються для їх автентифікації в ПТК НЕДП.
Строк чинності особистого ключа дорівнює строку чинності відповідного сертифіката ключа.

5.11.1. Порядок генерації ключів НЕДП

Генерація, зберігання, використання ключів НЕДП здійснюється виключно у засобах електронного підпису чи печатки, що забезпечують захист записаних даних від несанкціонованого доступу.
Резервні копії ключів НЕДП зберігаються у засобах електронного підпису чи печатки, що забезпечують захист записаних даних від несанкціонованого доступу.
Після закінчення строку дії сертифіката ключа НЕДП відповідний особистий ключ НЕДП та всі його резервні копії знищуються способом, що унеможливлюють їх відновлення.
Адміністратор сертифікації НЕДП відповідає за виконання процедур генерування та резервування ключів НЕДП. Генерування та резервування ключів НЕДП здійснюється за участі не менше трьох адміністраторів, а саме: адміністратора сертифікації, адміністратора безпеки та системного адміністратора. Резервування виконується тільки під час генерування ключів НЕДП на з'ємний носій інформації, що забезпечує захист записаних даних від несанкціонованого доступу.
Не менше ніж за два календарні роки до закінчення строку дії поточного особистого ключа НЕДП переходить на застосування нового особистого ключа НЕДП.
Адміністратор сертифікації за участю адміністратора безпеки здійснює генерацію таких пар ключів НЕДП, що використовуються для надання кваліфікованих електронних довірчих послуг:

- власні ключі НЕДП зі ступенем розширення основного поля еліптичної кривої не менше 431 згідно з ДСТУ 4145-2002;
- ключі OCSP-сервера зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;
- ключі TSP-сервера зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;
- ключі CMP-сервера зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;
- власні ключі НЕДП із використанням еліптичної кривої NIST P-256 для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2015;
- ключі OCSP-сервера із використанням еліптичної кривої NIST P-256 для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2015;
- ключі TSP-сервера із використанням еліптичної кривої NIST P-256 для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2015;
- ключі CMP-сервера із використанням еліптичної кривої NIST P-256 для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2015;
- власні ключі НЕДП для алгоритму RSA згідно RSA згідно з ISO/IEC 14888-2:2008 та PKCS#1;
- ключі OCSP-сервера для алгоритму RSA згідно з ISO/IEC 14888-2:2008 та PKCS#1 (довжина 4096 біт);
- ключі TSP-сервера для алгоритму RSA згідно з ISO/IEC 14888-2:2008 та PKCS#1 (довжина 4096 біт);
- ключі CMP-сервера для алгоритму RSA згідно з ISO/IEC 14888-2:2008 та PKCS#1 (довжина 4096 біт).

5.11.2. Порядок захисту та доступу до ключів НЕДП

Ключі НЕДП зберігаються виключно у засобах електронного підпису чи печатки, що забезпечують захист записаних даних від несанкціонованого доступу.
Для застосування ключів НЕДП необхідно ввести паролі доступу до засобу електронного підпису чи печатки.

5.12. Порядок та умови резервного копіювання особистого ключа НЕДП, збереження, доступу та використання резервних копій

Адміністратор сертифікації НЕДП створює резервні копії особистих ключів НЕДП за участю адміністратора безпеки. Адміністратор безпеки реєструє факти створення резервних копій особистих ключів НЕДП у відповідному журналі обліку.
Резервні копії особистих ключів НЕДП зберігаються у засобах електронного

підпису чи печатки, що забезпечують захист записаних даних від несанкціонованого доступу.
Особистий ключ НЕДП та всі його резервні копії після закінчення строку дії сертифіката ключа НЕДП знищуються способом, що унеможливлює їх відновлення. Адміністратор сертифікації здійснює знищення особистих ключів НЕДП та їх резервних копій за участю адміністратора безпеки.

5.13. Порядок та умови генерації пар ключів підписувачів

Відповідальні особи НЕДП забезпечують підписувача засобами електронного підпису чи печатки та надають йому допомогу під час генерування ключів у разі потреби. НЕДП надає допомогу підписувачу у спосіб, що не допускає порушення конфіденційності та цілісності особистого ключа підписувача, а також ознайомлення із значенням параметрів особистого ключа та їх копіювання.
Реєстрація підписувачів регламентується внутрішніми документами Банку.
НЕДП здійснює скасування реєстрації підписувача в такому порядку:
- адміністратор реєстрації НЕДП інформує, засобами внутрішніх комунікацій банку, адміністратора сертифікації НЕДП щодо необхідності зміни статусу зареєстрованого підписувача на "анульований";
- адміністратор сертифікації НЕДП скасовує сертифікат підписувача, формує СВС та поширює його в порядку, визначеному цим Регламентом.

5.13.1. Місце генерації ключів підписувачів

Відкритий та особистий ключі підписувача можуть бути згенеровані:
- на робочому місці підписувача;
- на робочих станціях генерації ключів НЕДП та ВПР (тільки для підписувачів, що є клієнтами Банку).

Заявник генерує ключі підписувача на робочій станції генерування ключів, яка входить до складу ПТК НЕДП, якщо підписувач надав йому відповідні повноваження.
Підписувач, який є працівником банку, самостійно генерує власні криптографічні ключі на своєму робочому місці.
НЕДП забезпечує:
- створення умов для генерації пари ключів підписувача;
- захист інформації з обмеженим доступом під час обміну інформацією між підписувачем та НЕДП.

5.13.2. Зберігання особистого ключа підписувача на НКІ та відповідальність

В НЕДП використовуються апаратно-програмні та програмні носії ключової інформації (НКІ), що відповідають вимогам законодавства України у сфері електронних довірчих послуг (для зберігання особистих ключів електронного підпису).
Згенерований особистий ключ підписувача захищається паролем та зберігається на НКІ. Підписувач несе відповідальність за забезпечення конфіденційності та цілісності особистого ключа, а також неможливості доступу до особистого ключа підписувача інших осіб. НЕДП несе відповідальність за забезпечення конфіденційності та цілісності особистого ключа підписувача, а також неможливості доступу до особистого ключа підписувача інших осіб у разі зберігання особистого ключа підписувача в HSM НЕДП (централізоване «хмарне» сховище ключів в мережевому апаратному модулі безпеки).
Генерацію та/або управління парою ключів від імені підписувача може здійснювати виключно НЕДП. Під час управління парою ключів підписувача НЕДП може здійснювати резервне копіювання особистого ключа підписувача з метою його зберігання за умови дотримання вимоги, що рівень безпеки резервної копії особистого ключа повинен відповідати рівню безпеки основного особистого ключа.

5.14. Механізм отримання підписувачем, який є клієнтом Банку, особистого ключа в результаті надання електронної довірчої послуги НЕДП

У разі використання підписувачем засобу електронного підпису чи печатки, фактичне отримання особистого ключа відбувається у момент генерації особистого ключа. У разі надання підписувачу доступу до частини ресурсу засобу електронного підпису чи печатки, який знаходиться у НЕДП, особистий ключ підписувача зберігається у зазначеному засобі електронного підпису чи печатки. Підписувач отримує доступ до свого особистого ключа за його запитом після процедури автентифікації підписувача.
У випадку генерації та зберігання особистого ключа підписувача на HSM, підписувач отримує виключний доступ до особистого ключа, що знаходиться на HSM НЕДП, за своїм запитом після проходження процедури двофакторної автентифікації.

5.15. Механізм надання клієнтом запиту на формування сертифіката ключа до НЕДП для формування сертифіката ключа

Під час генерації пари ключів засобами електронного підпису чи печатки формується запит у стандартному форматі PKCS#10 та підписується удосконаленим електронним підписом з використанням особистого ключа, що відповідає відкритому ключу із згенерованої пари ключів. Процес подання запиту на формування сертифіката ключа описаний у положеннях сертифікаційних практик цього Регламенту.

6. ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

6.1. Процес подання запиту на формування сертифіката ключа[3]

Запити на формування сертифіката ключа можуть подати наступні клієнти Банку:

- фізичні особи, що бажають отримати сертифікат ключа;
- юридичні особи (фізичні особи – підприємці), що бажають отримати сертифікат ключа, в особі їх посадових осіб.

НЕДП здійснює формування сертифікатів ключів підписувачів у такому порядку.

Адміністратор (оператор) реєстрації НЕДП (ВПР) опрацьовує поданий клієнтом Банку запит на формування сертифікату підписувача і заяву про формування сертифіката протягом 1 робочого дня з моменту надходження (у разі реєстрації клієнта Банку перевіряється також наявність всіх необхідних правильно оформлених документів, передбачених цим Регламентом).

Адміністратор сертифікації НЕДП формує сертифікати підписувача в разі позитивного рішення служби реєстрації НЕДП.

Адміністратор сертифікації НЕДП під час формування сертифікату підписувача:

- вносить до сертифіката підписувача обов'язкові дані, визначені чинним законодавством;
- вносить до сертифіката підписувача додаткові дані за зверненням підписувача;
- забезпечує унікальний реєстраційний номер підписувача, унікальність реєстраційного номера сертифіката в межах НЕДП, а також унікальність відкритих ключів у реєстрі чинних, блокованих та скасованих сертифікатів.

Адміністратор сертифікації НЕДП здійснює поширення сертифіката підписувача в установленому цим Регламентом порядку.

Порядок та умови формування сертифікатів ключів підписувачів, які є працівниками Банку, визначаються внутрішніми інструкціями Банку, затвердженими керівником НЕДП.

6.2. Порядок надання сформованого сертифіката ключа підписувачу

Після формування, сертифікат ключа автоматично публікується на Веб-порталі НЕДП.

Після отримання сертифікату ключа підписувач повинен перевірити

[3] перелік суб'єктів, уповноважених подавати запит на формування сертифіката ключа, порядок подачі та оброблення такого запиту, строки оброблення запиту на формування сертифіката ключа

достовірність даних, що містяться в сертифікаті. У разі виявлення розбіжностей між даними, що подавались для формування сертифікату ключа, та даними, що містяться у сертифікаті, підписувач повідомляє про це НЕДП, який вживає заходи щодо формування нового сертифікату ключа з обов'язковим скасуванням сертифікату ключа з виявленими розбіжностями.
Підписувач має право використовувати особистий ключ тільки після проведення перевірки своїх ідентифікаційних даних, внесених до відповідного сертифіката ключа. Використання підписувачем особистого ключа є фактом визнання ним відповідного сертифіката ключа.

6.3. Порядок та умови публікації сформованого сертифіката ключа клієнта на Веб-порталі НЕДП

Сформований сертифікат ключа автоматично стає доступним на Веб-порталі НЕДП.

6.4. Умови використання сертифіката ключа підписувача та його особистого ключа[4]

Підписувач несе відповідальність за безпосереднє надійне збереження особистого ключа (НКІ, на якому він знаходиться), а також пароля доступу до цього НКІ.
Підписувач несе відповідальність за забезпечення конфіденційності паролю доступу до особистого ключа на HSM НЕДП (у разі використання).
Користувачі електронних довірчих послуг зобов'язані дотримуватись наступних умов використання особистих ключів та сертифікатів ключів:
- забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;
- невідкладно повідомляти НЕДП про підозру або факт компрометації особистого ключа;
- надавати НЕДП достовірну інформацію, необхідну для отримання електронних довірчих послуг;
- своєчасно здійснювати оплату за електронні довірчі послуги, якщо така оплата передбачена договором між НЕДП та підписувачем;
- своєчасно надавати НЕДП інформацію про зміну ідентифікаційних даних, які містить сертифікат ключа;
- не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування сертифіката ключа.

Наслідками неправильного використання сертифіката ключа та особистого

[4] попередження про можливі наслідки неправильного використання сертифіката ключа та особистого ключа

ключа можуть стати недостовірна автентифікація підписувача в інформаційних системах, заволодіння зловмисниками правами доступу підписувача до інформації, підробка електронних документів, матеріальні та репутаційні втрати підписувача.

6.5. Процедура подачі запиту на формування сертифіката ключа для підписувачів, які мають чинний сертифікат ключа, сформований НЕДП

В разі, якщо підписувач має чинний сертифікат ключа, строк дії якого закінчується, він може автоматично отримати новий сертифікат ключа, згенерувавши нову ключову пару, сформувавши та надіславши до НЕДП новий запит на формування сертифіката, підписаний з використанням чинного особистого ключа.

Обробка запиту на формування сертифіката ключа здійснюється програмними засобами ПТК НЕДП 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 на формування сертифіката ключа передбачає встановлення (ідентифікації) особи клієнта Банку та підтвердження володіння клієнтом Банку особистим ключем, відповідний якому відкритий ключ надається для формування сертифіката відкритого ключа. Формування нового сертифіката відкритого ключа для клієнтів Банку, які мають чинний сертифікат відкритого ключа, попередньо сформований НЕДП, здійснюється за таких умов:

- сертифікат відкритого ключа клієнта Банку чинний;
- реєстраційні дані, які містяться у чинних сертифікатах відкритих ключів не змінилися;
- особистий ключ відповідний до чинного сертифіката відкритого ключа не скомпрометований.

Реквізити клієнта Банку, що вносяться до нового сертифіката ключа, імпортуються з попереднього сертифіката ключа клієнта Банку.

Автентифікація клієнта Банку виконується шляхом перевірки електронного підпису чи печатки клієнта Банку на відповідному запиті.

Клієнт Банку шляхом підписання запиту засвідчує, що його реєстраційні дані залишаються незмінними та приєднується до договору про надання електронних довірчих послуг на строк дії нового сертифіката ключа. Після успішного формування нового сертифіката відкритого ключа, попередній сертифікат може скасуватись в автоматичному режимі.

Якщо клієнт має чинний сертифікат відкритого ключа та звернувся до НЕДП особисто, в цьому випадку документи на формування нового сертифікату

подаються відповідно до цього Регламенту, а запит – відповідно до вимог цього Регламенту.
У разі неможливості доступу до власного ключа, підписувач повинен надати до НЕДП заяву про скасування його чинного сертифікату.
Якщо закінчився строк дії сертифіката ключа, сформованого НЕДП, підписувач подає заяву про формування нового сертифіката ключа і документи відповідно до вимог цього Регламенту.
Заява про формування нового сертифіката ключа і документи відповідно до вимог цього Регламенту, передаються із забезпеченням цілісності та конфіденційності інформації.

6.6. Порядок та умови блокування, поновлення, скасування сертифікатів ключів підписувачів

Надавач блокує, поновлює, скасовує сертифікати ключів клієнтів у випадках, визначених статтею 25 Закону України «Про електронні довірчі послуги» (далі – Закон).

6.6.1. Перелік суб'єктів, уповноважених подавати заяву на скасування (блокування, поновлення) сертифіката ключа

Уповноваженими на подання заяви на скасування (блокування, поновлення) сертифіката ключа є підписувачі (заявники).
Інші фізичні/юридичні особи мають право подавати документи, що підтверджують інформацію, передбачену статтею 25 Закону, у формі паперових документів або у формі електронних документів.

6.6.2. Процедура подання заяви на скасування (блокування, поновлення) сертифіката ключа

6.6.2.1. Загальні відомості щодо скасування (блокування, поновлення) сертифіката

Блокування сертифіката тимчасово припиняє дію сертифіката ключа.
Сертифікат ключа, статус якого змінено на заблокований, у період блокування не використовується.
Скасування сертифіката припиняє дію сертифікату ключа. Скасовані сертифікати поновленню не підлягають.
Поновлення чинності сертифікату ключа можливе лише для сертифікатів, що заблоковані і строк дії, зазначений у сертифікаті ключа, не закінчився.
Підписувач зобов'язаний подавати заяви про блокування, поновлення,

скасування сертифікатів ключів відповідно до вимог пункту 5.7 цього Регламенту.

6.6.2.2. Порядок блокування сертифіката ключа

Блокування сертифіката здійснюється НЕДП на підставі заяви, що надходить від підписувача установленим порядком в НЕДП в усній, паперовій формі чи у вигляді електронного документа або на підставі іншої причини, зазначеної у цьому Регламенті.
Сертифікат ключа вважається заблокованим з моменту зміни НЕДП статусу сертифіката ключа на заблокований.

6.6.2.3. Порядок скасування сертифіката ключа

Скасування сертифіката здійснюється НЕДП на підставі заяви, що надходить від підписувача установленим порядком в НЕДП в паперовій формі чи у вигляді електронного документа або на підставі іншої причини, зазначеної у цьому Регламенті.
Заява на скасування сертифіката засвідчується відповідно до цього Регламенту.
Електронна заява подається до НЕДП за встановленою формою та засвідчується підписувачем (заявником) за допомогою свого особистого ключа (якщо відповідний сертифікат ключа є чинним) і електронною печаткою організації (в разі наявності і у випадку клієнта – юридичної особи).
У випадку, якщо необхідне термінове скасування сертифіката ключа через об'єктивні обставини, з метою недопущення майнової шкоди, підписувач (заявник) має заблокувати сертифікат такого особистого ключа в усній формі з подальшим поданням письмової заяви про скасування сертифіката ключа.
Сертифікат ключа вважається скасованим з моменту зміни НЕДП статусу сертифіката ключа на скасований.

6.6.2.4. Порядок поновлення сертифіката ключа

Поновлення чинності сертифікату ключа можливе лише для сертифікатів, що заблоковані і строк дії сертифіката не скінчився. Скасовані сертифікати поновленню не підлягають.
Поновлення чинності сертифіката здійснюється НЕДП на підставі заяви, що надходить встановленим порядком в НЕДП в паперовій формі або у вигляді електронного документу.
Сертифікат ключа вважається поновленим з моменту зміни НЕДП статусу сертифіката ключа на чинний.

6.6.2.5. Час оброблення запитів на блокування, поновлення, скасування кваліфікованих сертифікатів ключів підписувачів

НЕДП здійснює прийом та перевірку заяв підписувачів про скасування, блокування, поновлення сертифікатів ключів підписувачів тільки в робочий час, відповідно до розпорядку роботи НЕДП. НЕДП скасовує, блокує та поновлює сертифікати ключів клієнтів не пізніше ніж протягом двох годин від часу реєстрації заяв про скасування, блокування, поновлення сертифікатів ключів підписувачів або реєстрації документів, що підтверджують інформацію, передбачену статтею 25 Закону.

6.6.3. Порядок та умови блокування, поновлення, скасування сертифікатів ключів підписувачів, які є працівниками Банку

Підписувач, що є працівником Банку, подає документи, передбачені цим Регламентом:

- у формі паперового документа за адресою НЕДП;
- у формі електронних документів через систему електронного документообігу, систему електронної пошти або систему обслуговування користувачів Банку.

6.7. Порядок та умови надання інформації про статус сертифікатів ключів, сформованих НЕДП

НЕДП поширює інформацію про статус сертифіката ключа:

- за запитом підписувача у реальному часі (OCSP-запити) з використанням OCSP-сервера НЕДП;
- шляхом поширення СВС.

Якщо одержати інформацію про статус сертифіката ключа підписувача тимчасово неможливо, то потрібно відмовитися від використання ключа.

6.7.1. Частота формування списку відкликаних сертифікатів та строки його дії

Публікація списків відкликаних сертифікатів на Веб-порталі НЕДП здійснюється у порядку, визначеному цим Регламентом.

НЕДП під час формування СВС забезпечує таке:

- наявність у СВС даних щодо часу формування наступного СВС;
- накладення ЕП на СВС за допомогою особистого ключа НЕДП.

НЕДП поширює СВС шляхом їх розміщення на Веб-порталі НЕДП.

Періодичність формування та поширення СВС:
- один раз на тиждень, навіть якщо за час від останнього формування СВС до нього не вносилися зміни, або
- протягом двох годин після отримання заяви про зміну статусу сертифіката ключа підписувача, або
- протягом однієї години після прийняття рішення про зміну статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа.

Наступний СВС може бути сформований раніше визначеного часу його формування.

6.7.2. Відомості про можливість та умови надання інформації про статус сертифіката ключа у режимі реального часу

Розповсюдження інформації про статус сертифіката ключа підписувача здійснюється також шляхом створення можливості перевірки статусу сертифіката ключа підписувача в режимі реального часу через телекомунікаційні мережі загального користування із використанням протоколу OCSP.

Посилання на сервіс перевірки статусу сертифіката ключа клієнта в режимі реального часу вносяться до сертифікатів ключів клієнтів.

Взаємодія з OCSP-сервером для отримання послуг визначення статусу сертифікатів ключів забезпечується шляхом використання клієнтського програмного забезпечення. Таке ПЗ повинно відповідати технічним специфікаціям та форматам даних, визначеним законодавством України у сфері електронних довірчих послуг. Підписувач на свій розсуд може використовувати клієнтське ПЗ, яке вільно поширюється шляхом його розміщення на Веб-порталі НЕДП, розроблене самостійно чи створене сторонніми розробниками.

6.8. Строки дії сертифікатів ключів, сформованих НЕДП

Строки дії сертифікатів відкритих ключів:
- сертифікат ключа послуги визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP – не більше ніж 5 років;
- сертифікат ключа послуги передачі користувачам сертифікатів в інтерактивному режимі за протоколом CMP – не більше ніж 5 років;
- сертифікат ключа посадової особи НЕДП – не більше ніж 2 роки;
- сертифікат ключа підписувача – не більше ніж 2 роки.

Дата, час початку та дата, час закінчення строку дії сертифіката ключа, сформованого НЕДП, зазначається у сертифікаті ключа із точністю до однієї секунди.

7. ПРОЦЕДУРИ ТА ПРОЦЕСИ, ЯКІ ВИКОНУЮТЬСЯ ПІД ЧАС НАДАННЯ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, ЩО НЕ ПЕРЕДБАЧАЮТЬ ФОРМУВАННЯ ТА ОБСЛУГОВУВАННЯ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ

7.1. Надання засобів електронного підпису чи печатки

НЕДП для надання електронних довірчих послуг використовуються засоби електронного підпису чи печатки.
Надання НЕДП клієнтам Банку засобів електронного підпису чи печатки у вигляді апаратно-програмних засобів (доступів, у випадку зберігання особистих ключів в HSM) та їх технічна підтримка і обслуговування здійснюється на договірних засадах.
Надання НЕДП засобів електронного підпису чи печатки може здійснюватися шляхом надання доступу до відповідних сервісів через Веб-портал НЕДП.
У випадку використання HSM НЕДП. Згенерований в HSM особистий ключ підписувача захищається паролем та зберігається в HSM. Доступ до зазначеного особистого ключа має лише підписувач. Підписувач несе відповідальність за забезпечення конфіденційності паролю доступу до особистого ключа. Під час кожного використання особистого ключа підписувачем, підписувач, після проведеної успішної двохфакторної автентифікації, делегує застосування свого особистого ключа НЕДП для створення електронного підпису та інших криптографічних операцій (розшифрування, автентифікації).

7.2. Надання електронної довірчої послуги формування, перевірки та підтвердження електронної позначки часу

Підписувачам надається електронна довірча послуга з формування, перевірки та підтвердження електронної позначки часу.
Послуги TSP надаються НЕДП з використанням TSP-сервера НЕДП.
Взаємодія з TSP-сервером НЕДП для отримання послуг TSP забезпечується шляхом використання клієнтського ПЗ. Таке ПЗ повинно відповідати технічним специфікаціям та форматам даних, визначеним законодавством України у сфері електронних довірчих послуг. Підписувач на свій розсуд може використовувати клієнтське ПЗ, яке поширюється шляхом його розміщення на Веб-порталі НЕДП, розроблене самостійно чи створене сторонніми розробниками.
Електронна довірча послуга формування, перевірки та підтвердження електронної позначки часу включає:

- формування електронної позначки часу;

- передачу електронної позначки часу користувачеві електронної довірчої послуги.

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

7.3. Синхронізація часу в ПТК НЕДП

Час, який використовується в позначці часу, установлюється з точністю до однієї секунди на момент формування позначки за київським часом, який синхронізований із всесвітнім координованим часом (UTC).

ПТК НЕДП забезпечує синхронізацію із всесвітнім координованим часом (UTC) з точністю до однієї секунди за допомогою мережевого протоколу NTP.

Алгоритм корекції часу в ПТК НЕДП з використанням NTP включає внесення затримок, корекцію частоти годинника і ряд механізмів, що дають змогу досягти необхідної точності під час синхронізації часу в ПТК НЕДП, навіть після тривалих періодів втрати зв'язку із сервером часу. ПТК НЕДП працює за київським часом з автоматичною поправкою на літній та зимовий періоди.

Системний адміністратор ЦСК налаштовує NTP з використанням засобів операційної системи.

7.4. Необхідні вимоги до процедур

НЕДП встановлює вимоги до процедур з управління ризиками, персоналом, інформаційною безпекою, інцидентами, доказами та архівами, поводження з персональними даними користувачів, процедур встановлення клієнтів Банку, опису фізичного середовища.

Зазначені вимоги затверджуються Регламентом та/або окремими документами НЕДП.