ПОГОДЖЕНО
Керівник засвідчувального центру

_____ І.В.Коновалов

"25" травня 2021 р.

ЗАТВЕРДЖУЮ
Голова Правління
АТ "БАНК АЛЬЯНС"

_____ Ю.М. Фролова

"28" травня 2021 р.

РЕГЛАМЕНТ РОБОТИ КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ АКЦІОНЕРНОГО ТОВАРИСТВА "БАНК АЛЬЯНС"

2021

ЗМІСТ

С.

ВСТУП

Цей документ є нормативним документом, що визначає організаційно-методологічні та технологічні умови діяльності кваліфікованого надавача електронних довірчих послуг АКЦІОНЕРНОГО ТОВАРИСТВА "БАНК АЛЬЯНС", (далі – КНЕДП) під час надання кваліфікованих електронних довірчих послуг та є регламентом роботи КНЕДП (далі – Регламент).

Цей Регламент визначає умови надання послуг та правил користування послугами КНЕДП, а також основні організаційно-технічні заходи, що направлені на забезпечення функціонування КНЕДП.

Регламент розроблено відповідно до чинного законодавства України у сфері електронних довірчих послуг.

Вимоги даного Регламенту є обов’язковими для виконання персоналом КНЕДП та підписувачами, а також служать засобом офіційного повідомлення і інформування усіх суб’єктів у взаєминах, що виникають в процесі надання і використання електронних довірчих послуг, що надаються КНЕДП.

Суб’єктами правових відносин у сфері електронних довірчих послуг, що обумовлюються цим регламентом є ЗЦ, КНЕДП і підписувачі.

Будь-яка заінтересована особа може ознайомитися з положеннями Регламенту на електронному інформаційному ресурсі, в офісах КНЕДП та його відокремлених пунктах реєстрації.

Застосування положень Регламенту засноване на його добровільному визнанні взаємодіючими сторонами. Добровільне визнання цього Регламенту іншою стороною є підставою для укладення договору (угоди) про взаємодію і надання відповідних послуг.

ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

БД – база даних КНЕДП, у якій зберігаються реєстр КНЕДП, інформаційно-довідкова, технологічна та інша службова інформація, потрібна для функціонування програмно-технічного комплексу (далі – ПТК) КНЕДП;

ВІДОКРЕМЛЕНИЙ ПУНКТ РЕЄСТРАЦІЇ – представництво (філія, підрозділ, територіальний орган) КНЕДП, що здійснює реєстрацію підписувачів з дотриманням вимог чинного законодавства;

ВІДПОВІДАЛЬНА ОСОБА КНЕДП – керівник КНЕДП, заступник керівника КНЕДП або адміністратори (оператори) КНЕДП, визначені у пункті 4 даного Регламенту;

ДОГОВІР, ВІДПОВІДНО ДО ЯКОГО ПІДПИСУВАЧУ НАДАЮТЬСЯ ЕЛЕКТРОННІ ДОВІРЧІ ПОСЛУГИ – окремий договір між підписувачем, який є клієнтом АТ "БАНК АЛЬЯНС" (далі – Банк), та АТ "БАНК АЛЬЯНС" про надання електронних довірчих послуг або договір про обслуговування клієнта банку, що має містити договір про надання електронних довірчих послуг підписувачу. Підписувачі, які є працівниками банку, не укладають з КНЕДП договір про надання електронних довірчих послуг;

ЗАЯВНИК – уповноважений представник підписувача, який є клієнтом банку, який на законних підставах звертається до КНЕДП з метою організації та проведення реєстрації підписувача – клієнта банку, отримання послуг від КНЕДП, а також зміни його даних (реквізитів) в установленому порядку. Якщо в основних даних (реквізитах) кваліфікованого сертифіката відкритого ключа (далі – сертифікат, сертифікат ключа) підписувача, який є клієнтом банку, сформованого за зверненням заявника, зазначаються реквізити заявника, то заявник і підписувач, який є клієнтом банку, є одним суб'єктом;

ЗМІНА ІДЕНТИФІКАЦІЙНИХ ДАНИХ ПІДПИСУВАЧА – зміна даних підписувача, що внесені до сертифіката підписувача, які попередньо надавалися заявником до КНЕДП;

ЗМІНА СТАТУСУ СЕРТИФІКАТА КЛЮЧА – виконання однієї з процедур блокування/скасування/поновлення сертифіката;

ІНФОРМАЦІЙНИЙ РЕСУРС КНЕДП – загальнодоступна частина БД. Доступ до інформаційного ресурсу КНЕДП є вільним і забезпечується через телекомунікаційні мережі загального користування;

ПІДПИСУВАЧ, ЯКИЙ Є КЛІЄНТОМ БАНКУ – клієнт банку, якому КНЕДП надає електронні довірчі послуги (далі – клієнт Банку). Банк укладає з підписувачем – клієнтом банку договір, відповідно до якого підписувачу надаються електронні довірчі послуги;

ПІДПИСУВАЧ, ЯКИЙ Є ПРАЦІВНИКОМ БАНКУ – працівник банку, який для виконання своїх службових обов'язків користується електронними довірчими послугами КНЕДП;

ПРОЦЕДУРА РЕЄСТРАЦІЇ ПІДПИСУВАЧА, ЯКИЙ Є КЛІЄНТОМ БАНКУ – установлена процедура подання заявником до КНЕДП необхідного пакета документів, опрацювання в КНЕДП цих документів і внесення відомостей про підписувача – клієнта банку до РЕЄСТРУ КНЕДП;

РЕЄСТР КНЕДП – електронна база даних, яка ведеться КНЕДП 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».

ПОЗНАЧКИ ТА СКОРОЧЕННЯ

ВПР - відокремлений пункт реєстрації;
ПТК - програмно-технічний комплекс;
СВС - список відкликаних сертифікатів;
ЗЦ - засвідчувальний центр;
ЦОД - центр обробки даних;
КНЕДП - кваліфікований надавач електронних довірчих послуг;
HSM - мережевий криптографічний модуль;
OCSP - Online Certificate Status Protocol (протокол визначення статусу сертифіката ключа);
НКІ - носій ключової інформації;
ПЗ - програмне забезпечення;
HTTP - протокол прикладного рівня, що використовується для передавання гіпертексту.

1 ЗАГАЛЬНІ ВІДОМОСТІ ПРО КНЕДП

1.1 Ідентифікаційні дані КНЕДП

Повне найменування Банку	АКЦІОНЕРНЕ ТОВАРИСТВО "БАНК АЛЬЯНС"
Код ЄДРПОУ Банку	14360506
Повне найменування КНЕДП	Кваліфікований надавач електронних довірчих послуг АКЦІОНЕРНОГО ТОВАРИСТВА "БАНК АЛЬЯНС"
Місцезнаходження КНЕДП	01010, м. Київ, вул. Московська, буд. 32/2
Юридична адреса КНЕДП	04053, м. Київ, вул. Січових Стрільців, буд. 50
Номери телефонів	+38 (044) 224-66-70
Електронна пошта	csk@ bankalliance.ua/
Електронна адреса	https://ca.bankalliance.ua
Режим роботи	Понеділок-П'ятниця – 09.00-18.00, Обідня перерва: 13.00-14.00

2 ПЕРЕЛІК ІНФОРМАЦІЇ, ЩО РОЗМІЩУЄТЬСЯ КНЕДП НА ЕЛЕКТРОННОМУ ІНФОРМАЦІЙНОМУ РЕСУРСІ КНЕДП

Електронний інформаційний ресурс КНЕДП призначено для розміщення на ньому відкритої інформації.

На електронному інформаційному ресурсі КНЕДП розміщується наступна інформація:

- відомості про КНЕДП;
- відомості про ВПР;
- сертифікати ключів КНЕДП;
- перелік електронних довірчих послуг, які надає КНЕДП;
- дані про засоби електронного підпису чи печатки, які КНЕДП надає клієнтам Банку (у разі коли електрона довірча послуга передбачає використання засобу електронного підпису чи печатки);
- форми документів, на підставі яких надаються електронні довірчі послуги;
- реєстр чинних, блокованих та скасованих сертифікатів ключів;
- відомості про обмеження під час використання сертифікатів ключів, сформованих КНЕДП;
- інформація про порядок перевірки чинності сертифіката ключа;
- зразок договору про надання електронних довірчих послуг клієнтам Банку;
- положення чинного регламенту роботи КНЕДП, засвідчені кваліфікованим електронним підписом уповноваженої особи КНЕДП;
- нормативно-правові акти України у сфері електронних довірчих послуг;
- довідково-методичні матеріали щодо порядку використання електронних довірчих послуг;

Електронний інформаційний ресурс КНЕДП доступний цілодобово.

Технічною основою інформаційного ресурсу КНЕДП є вебсервер, що входить до складу ПТК КНЕДП.

Довідкова інформація (регламент роботи КНЕДП, довідково-методичні матеріали щодо порядку використання електронних довірчих послуг, контактна інформація тощо) розміщується на вебсервері у вигляді набору вебсторінок або електронних документів.

3 ПЕРЕЛІК КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, НАДАННЯ ЯКИХ ЗАБЕЗПЕЧУЄ КНЕДП

1) кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки;

2) кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;

3) кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу.

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

4.1. Адміністратор (оператор) реєстрації відповідає за:

1) ідентифікацію, автентифікацію, верифікацію клієнтів Банку;

2) надання допомоги підписувачам під час генерації пар ключів (у разі необхідності);

3) опрацювання документів і запитів, наданих клієнтами.

Оператори реєстрації виконують обов'язки з реєстрації клієнтів Банку у відокремлених пунктах реєстрації.

4.2. Адміністратор сертифікації відповідає за:

- формування сертифікатів ключів;
- ведення реєстру чинних, блокованих та скасованих сертифікатів ключів;
- генерацію, створення резервних копій, використання особистих ключів КНЕДП;
- зберігання особистих ключів і резервних копій особистих ключів КНЕДП.

4.3. Системний адміністратор відповідає за належне функціонування програмно-технічного комплексу КНЕДП.

4.4. Адміністратор безпеки відповідає за належне функціонування комплексної системи захисту інформації.

Адміністратор безпеки відповідає за проведення перевірок дотримання адміністраторами (операторами) реєстрації, адміністраторами сертифікації, системними адміністраторами положень внутрішньої організаційно-розпорядчої документації КНЕДП та документації щодо комплексної системи захисту інформації та/або системи управління інформаційною безпекою.

4.5. У КНЕДП створено робочу групу з захисту інформації, яка відповідає за виконання адміністративних, технічних і технологічних функцій КНЕДП:

- із захисту інформації (адміністратори безпеки);
- із сертифікації (адміністратори сертифікації);
- із реєстрації (адміністратори та оператори реєстрації);
- із системного адміністрування (системний та черговий системний адміністратори);
- центр приймання дзвінків (оператори Центру приймання дзвінків).

5 ПОЛІТИКА СЕРТИФІКАТА

5.1 Перелік сфер, в яких дозволяється використання сертифікатів ключів, сформованих КНЕДП

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

Кваліфікований електронний підпис, який перевіряється з використанням сертифікатів ключів, що формуються КНЕДП, 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 кваліфікованого електронного підпису чи печатки;
- автентифікація;
- узгодження ключів шифрування.

5.2 Обмеження щодо використання сертифікатів ключів, сформованих КНЕДП

Обмеження щодо використання сформованих КНЕДП сертифікатів ключів застосовуються у відповідності до положень цього Регламенту та діючого законодавства України.

КНЕДП 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.

5.3 Час і порядок публікації сертифікатів ключів та списків відкликаних сертифікатів

5.3.1 Інформація щодо формування сертифікатів ключів підписувачів та самі сертифікати ключів (за згоди їх власників на опублікування своїх сертифікатів) розміщуються на електронному інформаційному ресурсі КНЕДП безпосередньо після їх формування.

5.3.2 Публікація списків відкликаних сертифікатів здійснюється на електронному інформаційному ресурсі КНЕДП одразу після їх формування.

5.3.3 КНЕДП виконує формування списків відкликаних сертифікатів двох типів:

− повний список;

− частковий список.

Повний список формується один раз на добу та містить інформацію про всі сертифікати, сформовані в КНЕДП за допомогою власного особистого ключа КНЕДП, 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.

У списках відкликаних сертифікатів обов'язково зазначається точна дата та час публікації наступного списку відкликаних сертифікатів.

Новий список відкликаних сертифікатів може бути опублікований до визначеного часу видання наступного списку, вказаного у поточному списку відкликаних сертифікатів.

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

Відкритий ключ підписувача подається для формування сертифіката ключа виключно у вигляді самопідписаного відповідним йому особистим ключем запиту. Належність підписувачу особистого ключа, що відповідає відкритому ключу, наданому для формування сертифіката ключа, підтверджується шляхом перевірки в КНЕДП удосконаленого електронного підпису на запиті на формування сертифіката ключа.

Підтвердження володіння підписувачем особистим ключем здійснюється без розкриття особистого ключа.

5.5 Умови ідентифікації та верифікації клієнта Банку (документи, які клієнт Банку повинен надати для отримання електронних довірчих послуг, вимоги щодо особистої присутності клієнта Банку).

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

5.5.2 Ідентифікація фізичної особи, яка звернулася за отриманням кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого 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.

5.5.3 Допускається ідентифікація фізичної особи за ідентифікаційними даними, що містяться у раніше сформованому КНЕДП сертифікаті ключа, за умови чинності цього сертифіката.

5.5.4 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.

5.5.5 Під час перевірки цивільної правоздатності та дієздатності юридичної особи КНЕДП 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.

5.5.6 КНЕДП під час формування та видачі сертифіката ключа здійснює ідентифікацію особи уповноваженого представника юридичної особи відповідно до вимог пункту 5.5.2 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 КНЕДП подається документ, у якому визначено повноваження відповідного органу та розподіл обов’язків між його членами.

5.5.7 Реєстрація клієнта Банку – представника юридичної особи

Клієнт Банку (представник юридичної особи) під час проведення реєстрації в КНЕДП (ВПР) подає такі документи:

- заповнену заяву про формування сертифікату, підписану підписувачем та уповноваженою особою юридичної особи, засвідчену відбитком печатки (у разі наявності); у заяві обов’язково зазначається адреса, телефон або інша інформація, що дозволяє зв'язатися з підписувачем;

запит на формування сертифікату підписувача, згенерований відповідно до вимог п.6.1 цього Регламенту;

- копія документа про обрання (призначення, надання повноважень) уповноваженої особи юридичної особи, засвідчена в установленому порядку (надається тільки юридичною особою);

- копії 1-2 сторінок, 3-6 сторінок за наявності на них відміток з паспорту фізичної особи - підписувача, засвідчені в установленому порядку.

При наявності паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій з унікальним номером запису в Єдиному державному демографічному реєстрі, надається його копія з обох боків та копія витягу з Єдиного державного демографічного реєстру, засвідчені в установленому порядку. Для фізичних осіб-нерезидентів – копія посвідки на тимчасове чи постійне місце проживання, засвідчена в установленому порядку копія довідки про включення до Державного реєстру фізичних осіб-платників податків, засвідчена в установленому порядку;

- копія довідки про включення до Державного реєстру фізичних осіб-платників податків, засвідчена в установленому порядку.

Якщо через релігійні переконання фізична особа відмовилась від реєстраційного

номера облікової картки платника податків, додатково подається копія сторінки паспорту з відміткою про таку відмову, засвідчена в установленому порядку;

- копія документу, що підтверджує посаду підписувача, засвідчена в установленому порядку.

5.5.8 Реєстрація клієнта Банку – фізичної особи (фізичної особи – підприємця)

Клієнт Банку (фізична особа/фізична особа-підприємець) під час проведення реєстрації в КНЕДП (ВПР) подає такі документи:

- заява на формування сертифіката для фізичної особи (фізичної особи – підприємця), підписана фізичною особою (фізичною особою – підприємцем). У заяві обов'язково зазначається адреса, телефон або інша інформація, що дозволяє зв'язатися з ним;

запит на формування сертифікату підписувача, згенерований відповідно до вимог п.6.1 цього Регламенту;

- копії 1-2 сторінок, 3-6 сторінок за наявності на них відміток та сторінки, у якій вказано останнє місце реєстрації, з паспорту, засвідчені фізичною особою (фізичною особою – підприємцем). При наявності паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій з унікальним номером запису в Єдиному державному демографічному реєстрі, надається його копія з обох боків та копія Довідки про реєстрацію місця проживання особи. Для фізичних осіб-нерезидентів – копія посвідки на тимчасове чи постійне місце проживання, засвідчена в установленому порядку копія довідки про включення до Державного реєстру фізичних осіб-платників податків, засвідчена в установленому порядку;

- копія довідки про включення до Державного реєстру фізичних осіб-платників податків, засвідчена фізичною особою (фізичною особою – підприємцем).

Якщо через релігійні переконання фізична особа (фізична особа – підприємець) відмовилась від реєстраційного номера облікової картки платника податків, додатково подається копія сторінки паспорту з відміткою про таку відмову, засвідчена в установленому порядку.

5.5.9 Процедура реєстрації клієнта Банку

Реєстрація клієнта Банку, здійснюється в такому порядку.

Клієнт Банку відвідує КНЕДП (ВПР) для подання документів, зазначених у пунктах 5.5.7/5.5.8 цього Регламенту.

Адміністратор (оператор) реєстрації КНЕДП (ВПР) під час процедури реєстрації надає, за потреби, клієнту Банку носій ключової інформації та відповідне ПЗ на договірних засадах.

Адміністратор (оператор) реєстрації КНЕДП (ВПР) опрацьовує подані документи протягом 1 робочого дня з моменту їх надходження згідно з вимогами цього Регламенту У разі подання документів до ВПР, після опрацювання оператором реєстрації документи з ВПР передаються в центр реєстрації з дотриманням захисту від несанкціонованого доступу.

У разі наявності всіх необхідних правильно оформлених документів КНЕДП забезпечує внесення до реєстру КНЕДП необхідних даних підписувача згідно з вимогами цього Регламенту та забезпечує виконання дій, передбачених п. 6.1.

5.5.10 КНЕДП не приймає до розгляду документи, які мають підчистки, дописки, закреслені слова, інші незастережні виправлення або написи, а також пошкодження, внаслідок чого їхній текст не можна прочитати.

5.5.11 За результатами розгляду наданих документів адміністратор (оператор) реєстрації приймає рішення про відмову у реєстрації у наступних випадках:

- у разі подання неповного пакету документів, передбачених пп. 5.5.7/5.5.8 цього Регламенту;
- у разі невідповідності поданого пакету документів вимогам, встановленим КНЕДП;
- у разі подання неналежно засвідчених копій документів;
- у разі встановлення невідповідності наданих під час реєстрації даних фактичним;
- у разі ненадання запитів на формування сертифікатів ключів підписувачем (заявником).

5.5.12 У разі відмови у реєстрації, адміністратор (оператор) реєстрації повертає надані документи клієнту Банку з роз'ясненням причин повернення.

5.5.13 Особа, вважається встановленою, при одночасному виконанні наступних умов:

- відомості, зазначені у заяві на формування сертифіката ключа підписувача, збігаються із відповідними відомостями, наведеними в представлених документах;

- представлені документи відповідають вимогам, встановленим чинним законодавством та не містять ознак навмисного внесення змін до їх змісту (підчистки, затирання окремих місць, незавірені виправлення тощо).

5.5.14 У разі, якщо нормативно-правовими актами тимчасово встановлюються інші вимоги до певних видів документів, то на цей час будуть діяти відповідні норми прийнятих нормативно-правових актів без внесення додаткових змін до цього Регламенту.

5.6 Механізм автентифікації підписувачів, які мають чинний сертифікат ключа, сформований КНЕДП

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

- 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: кваліфікований електронний підпис, сформований з використанням особистого ключа підписувача.

5.7 Механізм автентифікації 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 правомочності 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 кваліфікованим електронним підписом, створеним за допомогою особистого ключа підписувача (у разі чинності відповідного сертифіката ключа підписувача) та кваліфікованої 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.

5.8 Фізичне середовище

5.8.1 Опис спеціального приміщення

5.8.1.1 Компоненти ПТК КНЕДП розміщуються у Центрі обробки даних (далі – ЦОД).

ПТК КНЕДП функціонує на базі основного ЦОД та резервного ЦОД.

Основний ЦОД розташований в межах центру обробки даних інформаційно-телекомунікаційної системи «Хмарний центр обробки даних ТОВ «ДЕ НОВО» за адресою: м. Київ, вул. Північно-Сирецька, 1-З.

Резервний ЦОД розташований в межах дата-парку «БІ МОБАЙЛ» за адресою: м. Київ, вул. Куренівська, 21-А.

Переключення між основним та резервними ЦОД виконується за відповідним регламентом.

Усі автоматизовані робочі місця (далі – АРМ) КНЕДП розміщуються в приміщеннях з обмеженим доступом за адресою: м. Київ, вул. Січових Стрільців, буд. 50 та м. Київ, вул. Московська, буд. 32/2.

АРМ операторів реєстрації розташовуються в контрольованій зоні приміщень ВПР.

5.8.1.2 Приміщення, в яких розміщені компоненти ПТК КНЕДП, відповідають вимогам техніки безпеки та протипожежної безпеки, комплектуються необхідними засобами енергозабезпечення, охоронної та протипожежної сигналізації, відеоспостереження (за необхідності), допоміжними технічними засобами (механічний замок у робочому приміщенні КНЕДП, механічний замок та електронний кодовий замок у спеціальному приміщенні КНЕДП), системами життєзабезпечення (кондиціонерами).

Пропускний і внутрішній режими визначаються внутрішніми інструкціями і передбачають порядок допуску співробітників і представників інших організацій на територію КНЕДП, порядок внесення і винесення матеріальних цінностей, а також виконання особами, що перебувають на території КНЕДП, встановлених вимог режиму й розпорядку робочого дня.

Відповідальність за організацію охорони, стан перепускного й внутрішнього режиму КНЕДП в цілому покладається на адміністраторів безпеки.

Загальне керівництво й контроль за організацією охорони, станом перепускного й внутрішнього режиму здійснює заступник керівника КНЕДП.

5.8.1.3 Основний та резервний ЦОД та приміщення з обмеженим доступом відповідають вимогам:

- Положення про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України, затвердженого постановою Правління Національного банку України № 265 від 17.06.2004 та зареєстрованого в Міністерстві юстиції України 09.07.2004 за № 857/9456 (зі змінами);
- Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджених постановою Правління Національного банку України № 243 від 04.07.2007 та зареєстрованих в Міністерстві юстиції України 17.08.2007 за № 955/14222 (зі змінами);
- наказу Адміністрації Держспецзв'язку від 14.05.2020 № 269 «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації»;
- Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України № 95 від 28.09.2017.

5.8.2 Механізми контролю доступу до ЦОД та приміщень з обмеженим доступом

5.8.2.1 Доступ до ЦОД у супроводі відповідальної особи за експлуатацію ЦОД (або іншої уповноваженої особи) та приміщень з обмеженим доступом у режимі штатної роботи КНЕДП мають:

- керівник КНЕДП;
- заступники керівника КНЕДП;
- адміністратор безпеки;
- системний адміністратор;
- адміністратор сертифікації.

5.8.2.2 Доступ до обладнання, на якому функціонує КНЕДП в ЦОД дозволений тільки в супроводі посадових осіб КНЕДП.

5.8.2.3 Доступ до обладнання, на якому функціонує КНЕДП в ЦОД інших осіб, окрім визначених вище, може здійснюватися коли виконуються усі наступні умови:

- відвідування здійснюється за погодженням керівника або заступника керівника КНЕДП;
- склад відвідувачів, час відвідування та план робіт, що будуть виконуватися у спеціальному приміщенні КНЕДП відвідувачами задокументовані та узгоджені з адміністратором безпеки;
- протягом усього часу знаходження відвідувачів у спеціальному приміщенні КНЕДП дії відвідувачів контролюються адміністратором безпеки.

5.8.2.4 Факти доступу до ЦОД та приміщень з обмеженим доступом інших осіб, окрім персоналу КНЕДП, повинні бути запротокольовані (з зазначенням мети і часу відвідування, складу відвідувачів, а також їхніх ідентифікаційних даних) та засвідчені підписом адміністратора безпеки або керівника КНЕДП.

5.9 Процедурний контроль (система дисциплінарних стягнень за недотримання відповідальними особами КНЕДП своїх обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації КНЕДП та документації на комплексну систему захисту інформації та/або систему управління інформаційною безпекою в межах організації з урахуванням режиму роботи КНЕДП).

У разі порушення або невиконання своїх обов'язків відповідальними особами КНЕДП Банком може бути розірвано з ними трудову угоду (контракт, договір) за ініціативою керівництва Банку згідно з чинним законодавством.

Порушення (невиконання) положень цього Регламенту може призвести до кримінальної, цивільної або адміністративної відповідальності згідно з чинним законодавством України у вигляді штрафу, зобов'язання з відшкодування нанесених збитків, іншої дисциплінарної відповідальності.

5.10 Порядок ведення журналів аудиту подій

5.10.1 Типи подій, що фіксуються у журналах аудиту подій

ПТК КНЕДП налаштований на реєстрацію наступних подій:

– спроби створення, знищення, встановлення паролів, зміни прав доступу в інформаційно-телекомунікаційній системі;

– заміна програмного забезпечення, технічних засобів інформаційно-телекомунікаційної системи;

– технічне обслуговування інформаційно-телекомунікаційної системи;

– генерація, використання, знищення особистих ключів КНЕДП;

– формування, блокування, скасування та поновлення сертифікатів ключів, формування списків відкликаних сертифікатів ключів;

– спроба несанкціонованого доступу до інформаційно-телекомунікаційної системи;

– надання доступу персоналу до інформаційно-телекомунікаційної системи;

– збої в роботі інформаційно-телекомунікаційної системи;

– інші події, необхідні для збору доказів.

Параметри реєстрації подій в ПТК КНЕДП (в електронній або паперовій формі):

– дата, час, тип події, результат (успішність/неуспішність) події;

– ідентифікатор підписувача (процесу), що ініціював подію.

Записи подій у журналах аудиту подій в паперовій формі підписуються адміністратором безпеки.

Адміністратор безпеки зобов'язаний вести журнали обліку, передбачені документацією на комплексну систему захисту інформації інформаційно-телекомунікаційної системи КНЕДП.

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 ПТК КНЕДП та в журналах аудиту подій в електронній формі, повинен бути синхронізований із Всесвітнім координованим часом із точністю до секунди.

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

5.10.2 Частота перегляду журналів аудиту подій

Журнали аудиту подій, що ведуться в ПТК КНЕДП, переглядаються адміністратором безпеки періодично, але не рідше одного разу на добу з метою виявлення сукупності подій (серед зареєстрованих у журналі аудиту), які свідчать про ситуацію, яка призвела або може призвести до порушення безпеки експлуатації комплексу.

Також під час перегляду журналів аудиту подій вивчаються зафіксовані події та перевіряється наявність несанкціонованої модифікації.

Адміністратор (оператор) реєстрації, адміністратор сертифікації, системний адміністратор зобов'язані:

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

- повідомляти адміністратора безпеки про наявність несанкціонованої модифікації в ІТС КНЕДП, виявлену під час перегляду журналів аудиту подій.

5.10.3 Строки зберігання журналів аудиту подій

Журнали аудиту подій, що ведуться в ПТК КНЕДП, зберігаються протягом 5 років з моменту внесення останнього запису, після чого забезпечується їх передача на архівне зберігання.

5.10.4 Порядок захисту та резервного копіювання журналів аудиту подій, сертифікатів ключів, списків відкликаних сертифікатів

Резервні копії журналів аудиту подій, сертифікатів ключів, списків відкликаних сертифікатів на з'ємних носіях зберігаються у віддаленому резервному пункті із забезпеченням їх захисту від несанкціонованого доступу.

Резервне копіювання журналів аудиту здійснюється раз на добу (на резервний сервер КНЕДП), резервне копіювання журналів аудиту на з'ємні носії здійснюється раз на тиждень.

Резервування здійснюється системним адміністратором відповідними засобами, що входять до складу операційної системи персонального комп'ютера, системи керування базами даних та засобами ПТК КНЕДП, під контролем та за участю адміністратора безпеки. Факти проведення резервування у КНЕДП протоколюються (за період) та засвідчуються підписами відповідальних осіб.

Управління доступом до резервних копій журналів аудиту та контроль за їх зберіганням та застосуванням здійснює адміністратор безпеки.

5.10.5 Перелік посад, що можуть здійснювати перегляд журналів аудиту

Відповідальні особи КНЕДП мають доступ до журналів аудиту лише своїх АРМів за допомогою власного АРМу та відповідного модулю перегляду журналів аудиту.

Перегляд та перевірку цілісності всіх журналів аудиту, що ведуться в ПТК КНЕДП, дозволяється здійснювати лише керівнику КНЕДП, його заступникам та адміністратору безпеки за допомогою відповідного модулю перегляду журналів аудиту.

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

Керівник КНЕДП, заступник керівника КНЕДП, адміністратор безпеки мають право переглядати всі журнали аудиту подій, які ведуться КНЕДП, в тому числі журнали обліку, передбачені документацією на КСЗІ в ІТС КНЕДП.

5.11 Порядок ведення, збереження (із зазначенням строків зберігання), резервування, відновлення, захисту даних, пов’язаних із формуванням та обслуговуванням КНЕДП сертифікатів ключів

КНЕДП забезпечує постійне зберігання усіх сформованих сертифікатів ключів, реєстрів сформованих сертифікатів ключів, СВС. КНЕДП забезпечує зберігання документів, на підставі яких клієнтам надавалися кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані сертифікати ключів, протягом строку, встановленого Правилами застосування переліку документів, що утворюються в діяльності Національного банку України та банків України, затвердженими постановою Правління Національного банку України від 27листопада 2018року № 130 (зі змінами).

5.11.1 Види інформації

У КНЕДП циркулює (приймається, обробляється, пересилається і зберігається) інформація, яка за режимом доступу поділяється на відкриту інформацію та інформацію з обмеженим доступом, що має гриф «банківська таємниця» та «конфіденційна інформація».

5.11.1.1 Відкрита інформація

Відкрита інформація може зберігатися на паперових носіях та в електронній формі.

Відкрита інформація в електронній формі може оприлюднюватися шляхом її розміщення на інформаційному ресурсі КНЕДП і розсилання засобами електронної пошти (e-mail) банку.

До відкритої інформації КНЕДП, яка потребує захисту (в частині забезпечення цілісності та доступності), належать:

- зміст цього Регламенту;
- нормативні документи та нормативно-довідкові матеріали;

- зразок договору про надання електронних довірчих послуг підписувачам, які є діючими або потенційними клієнтами Банку;

- сертифікати ключів, сформовані КНЕДП;

- інформація про статус сертифікатів, сформованих КНЕДП.

5.11.1.2 Інформація з обмеженим доступом у електронній формі

До інформації з обмеженим доступом КНЕДП у електронній формі належать:

- особисті ключі КНЕДП, особисті ключі відповідальних осіб КНЕДП і підписувачів,;

- інформація про підписувачів, що міститься у БД КНЕДП і не підлягає безпосередньому поширенню, як частина сертифіката;

- резервні копії БД;

- налаштування технічних і програмних засобів ПТК КНЕДП;

- зміст протоколів роботи ПТК КНЕДП.

5.11.1.3 Інформація з обмеженим доступом у паперовій/електронній формі

До інформації з обмеженим доступом КНЕДП у паперовій/електронній формі належать документи:

- що подаються до КНЕДП під час проведення процедур реєстрації, формування сертифікатів, зміни статусу сертифікатів, зміни ідентифікаційних даних підписувачів і не підлягають безпосередньому оприлюдненню;

- журнали аудиту подій;

- інструкції відповідальних осіб КНЕДП банку;

- інструкції щодо роботи з ключовими даними.

5.11.1.4 Доступ до інформації з обмеженим доступом

Доступ до інформації з обмеженим доступом КНЕДП мають відповідальні особи КНЕДП банку з дотриманням вимог інформаційної безпеки, визначених для КНЕДП.

Доступ до особистих ключів КНЕДП розподілено між адміністраторами КНЕДП згідно Методики захисту особистого ключа КНЕДП, погодженої з Державною службою спеціального зв'язку та захисту інформації України.

Доступ до особистих ключів, які КНЕДП використовує для створення позначки часу, та особистих ключів, які КНЕДП використовує для надання інформації про статус сертифіката ключа у режимі реального часу, має адміністратор сертифікації КНЕДП.

Доступ до особистих ключів відповідальних осіб КНЕДП та підписувачів мають виключно власники даних ключів.

Доступ до інформації з обмеженим доступом КНЕДП може бути надано іншим особам лише у випадках, передбачених законодавством України.

5.11.2 Типи документів та даних, що підлягають архівуванню

Архівному зберіганню підлягають наступні документи КНЕДП:

- сертифікати КНЕДП, відповідальних осіб КНЕДП та підписувачів (чинні, скасовані, блоковані);

- реєстр сформованих кваліфікованих сертифікатів відкритих ключів;

- реєстр КНЕДП;

- копії і оригінали документів на папері та/або в електронній формі, що подані підписувачами (заявниками) під час реєстрації (визначені у пунктах 5.5.7 та 5.5.8 цього Регламенту), формування, зміни статусу сертифіката, зміни даних підписувачів;

- СВС;

- журнали аудиту КНЕДП, у тому числі протоколи роботи ПТК КНЕДП.

5.11.3 Строки зберігання архівів

КНЕДП зберігає документовану інформацію та СВС протягом строків, визначених 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).

5.11.4 Механізми та порядок зберігання, захисту та знищення архівних документів

Архівні документи в електронному вигляді зберігаються на з'ємних носіях із забезпеченням їх захисту від несанкціонованого доступу.

Знищення архівних документів здійснюється у порядку, визначеному 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).

5.11.5 Умови надання архівної інформації

КНЕДП надає доступ до необхідного сертифіката та пов'язаних з ним СВС з архівних записів КНЕДП за запитом клієнтів Банку у строки, установлені законодавством України для відповідей на звернення громадян, а також в інших випадках, передбачених законодавством України.

5.12 Порядок та умови генерації, зберігання, використання пар ключів КНЕДП

5.12.1 Порядок генерації ключів КНЕДП

Генерація, зберігання, використання ключів КНЕДП здійснюється виключно у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу.

Резервні копії ключів КНЕДП зберігаються у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями (зокрема, з'ємними носіями інформації), що забезпечують захист записаних даних від несанкціонованого доступу.

Після закінчення строку дії сертифіката ключа КНЕДП відповідний особистий ключ КНЕДП та всі його резервні копії знищуються способом, що унеможливлюють їх відновлення.

Адміністратор сертифікації КНЕДП відповідає за виконання процедур генерування та резервування ключів КНЕДП. Генерування та резервування ключів КНЕДП здійснюється за участі не менше трьох адміністраторів, а саме: адміністратора сертифікації, адміністратора безпеки та системного адміністратора. Резервування виконується тільки під час генерування ключів КНЕДП на з'ємний носій інформації, який є апаратно-програмним або апаратним пристроєм, що забезпечує захист записаних даних від несанкціонованого доступу.

Не менше ніж за один календарний рік до закінчення строку дії поточного особистого ключа КНЕДП переходить на застосування нового особистого ключа КНЕДП завчасно згенерованого та відкритий ключ якого засвідчено в ЗЦ.

5.12.2 Порядок захисту та доступу до ключів КНЕДП

Ключі КНЕДП зберігаються виключно у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу.

Для застосування ключів КНЕДП необхідно ввести коди доступу до засобу кваліфікованого електронного підпису чи печатки.

5.13 Порядок та умови резервного копіювання особистого ключа КНЕДП, збереження, доступу та використання резервних копій

Резервне копіювання особистого ключа КНЕДП здійснюється виключно з використанням засобів кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу

Резервна копія особистого ключа КНЕДП може бути застосована лише за погодженням керівника КНЕДП або його заступників та лише за умов, коли основний особистий ключ КНЕДП було знищено з причин, не пов'язаних з його компрометацією, або вийшов з ладу засіб кваліфікованого електронного підпису чи печатки, в якому зберігався основний особистий ключ.

Застосування резервної копії особистого ключа КНЕДП здійснюється у такому ж порядку, як і використання основного особистого ключа КНЕДП, та здійснюється під контролем адміністратора безпеки.

Запечатаний тубус (контейнер), із носієм, що містить резервну копію особистого ключа КНЕДП, опечатаний адміністратором сертифікації, зберігається у сейфі керівника КНЕДП або заступника керівника КНЕДП.

Запечатаний та надписаний конверт із значенням кодів доступу до носія, що містить резервну копію особистого ключа КНЕДП, опечатаний адміністратором сертифікації, системним адміністратором та адміністратором безпеки, зберігається у сейфі керівника КНЕДП.

5.14 Порядок та умови генерації пар ключів підписувачів

Відповідальні особи КНЕДП (ВПР) забезпечують підписувача засобами кваліфікованого електронного підпису чи печатки та надають йому допомогу під час генерування ключів у разі потреби.

5.14.1 Місце генерації ключів підписувачів

Відкритий та особистий ключі підписувача можуть бути згенеровані:

- на робочому місці підписувача;
- в КНЕДП (ВПР) на робочій станції генерування ключів підписувачів (за наявності технічної можливості).

5.14.2 Зберігання особистого ключа підписувача на НКІ та відповідальність

В КНЕДП використовуються такі НКІ:

- апаратно-програмні носії (токен, HSM тощо), що відповідають вимогам законодавства України у сфері електронних довірчих послуг (для зберігання особистих ключів кваліфікованого електронного підпису).

Згенерований особистий ключ підписувача захищається паролем та записується на носій ключової інформації. Підписувач несе відповідальність за забезпечення конфіденційності та цілісності особистого ключа, а також неможливості доступу до особистого ключа підписувача інших осіб у разі зберігання особистого ключа підписувача на токені. КНЕДП 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.

5.15 Механізм отримання підписувачем, який є клієнтом Банку, особистого ключа в результаті надання електронної довірчої послуги КНЕДП

5.15.1. У випадку зберігання особистого ключа підписувача на токен, підписувач отримує особистий ключ на власний носій ключової інформації під час генерації ключів.

5.15.2. У випадку генерації та зберігання особистого ключа підписувача на HSM, підписувач отримує виключний доступ до особистого ключа, що знаходиться на HSM КНЕДП, за своїм запитом після проходження процедури двофакторної автентифікації.

5.16 Механізм надання клієнтом Банку запиту на формування сертифіката ключа до КНЕДП для формування сертифіката ключа

Клієнт Банку подає запит на формування сертифікату ключа під час реєстрації клієнта Банку відповідно до пункту 6.1 цього Регламенту.

Клієнт Банку, що має чинний сертифікат ключа, подає запит на формування сертифікату ключа відповідно до пункту 6.5 цього Регламенту.

6 ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

6.1 Процес подання запиту на формування сертифіката ключа (перелік суб'єктів, уповноважених подавати запит на формування сертифіката ключа, порядок подачі та оброблення такого запиту, строки оброблення запиту на формування сертифіката ключа)

6.1.1 Перелік суб'єктів, які можуть подавати запит на формування сертифіката ключа

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.

Клієнт Банку зобов'язаний разом із запитом на формування сертифіката ключа заяву на формування сертифіката.

6.1.2 КНЕДП здійснює формування сертифікатів ключів підписувачів у такому порядку

Адміністратор (оператор) реєстрації КНЕДП (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 п. 5.5.7/5.5.8).

Адміністратор сертифікації КНЕДП формує сертифікати підписувача в разі позитивного рішення Служби реєстрації КНЕДП.

Адміністратор сертифікації КНЕДП 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 КНЕДП, а також унікальність відкритих ключів у реєстрі чинних, блокованих та скасованих сертифікатів.

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

6.1.3 Порядок та умови формування сертифікатів ключів підписувачів, які є працівниками Банку, визначаються внутрішнім розпорядчим документом Банку.

6.2 Порядок надання сформованого сертифіката ключа підписувачу

Після формування сертифіката ключа, у разі надання дозволу на його публікацію, адміністратор сертифікації публікує сертифікат ключа на електронний інформаційний ресурс КНЕДП, а у разі ненадання дозволу на публікацію сертифіката ключа КНЕДП – надсилає його підписувачу іншими технічними каналами зв'язку (електронною поштою на адресу, зазначену у заяві на формування сертифіката ключа).

Після отримання сертифікату ключа підписувач повинен перевірити достовірність даних, що містяться в ньому. У разі виявлення розбіжностей між даними, що подавались для формування сертифікату ключа, та даними, що містяться у сертифікаті, підписувач повідомляє про це КНЕДП, який вживає заходи щодо формування нового сертифікату ключа з обов'язковим скасуванням сертифікату ключа з виявленими розбіжностями.

6.3 Порядок та умови публікації сформованого сертифіката ключа клієнта на електронному інформаційному ресурсі КНЕДП

В разі, якщо при формуванні сертифіката ключа підписувача він погодився на його опублікування, сформований сертифікат ключа автоматично стане доступним на електронному інформаційному ресурсі КНЕДП.

6.4 Умови використання сертифіката ключа підписувача та його особистого ключа (попередження про можливі наслідки неправильного використання сертифіката ключа та особистого ключа)

Відповідальність підписувача – власника сертифіката ключа під час використання особистого ключа та сертифіката ключа

Клієнт Банку (юридична особа) несе відповідальність за організацію надійного зберігання, а підписувач (посадова особа клієнта Банку) або підписувач (фізична особа) за безпосереднє надійне збереження особистого ключа та носія ключової інформації, на якому він знаходиться (у разі використання підписувачем токена), а також значення коду доступу до цього носія.

Підписувач несе відповідальність за забезпечення конфіденційності паролю доступу до особистого ключа на HSM.

Підписувач несе відповідальність за розповсюдження власного сертифікату ключа (якщо підписувач не дав згоду на його публікацію на електронному інформаційному ресурсі КНЕДП).

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

6.5.1. 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 КНЕДП новий запит на формування сертифіката, підписаний з використанням чинного особистого ключа.

Обробка запиту на формування сертифіката ключа здійснюється програмними засобами ПТК КНЕДП 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 кваліфікованого сертифіката відкритого ключа. Формування нового кваліфікованого сертифіката відкритого ключа для клієнтів Банку, які мають чинний кваліфікований сертифікат відкритого ключа, попередньо сформований КНЕДП, здійснюється за таких умов:

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

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

Автентифікація клієнта Банку виконується шляхом перевірки кваліфікованого 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 кваліфікованих електронних довірчих послуг на строк дії нового сертифіката ключа. Після успішного формування нового кваліфікованого сертифіката відкритого ключа, попередній скасовується в автоматичному режимі.

Якщо клієнт має чинний кваліфікований сертифікат відкритого ключа та звернувся до КНЕДП (ВПР) особисто, в цьому випадку документи на формування нового кваліфікованого сертифікату подаються відповідно до вимог п. 5.5.7/5.5.8 цього Регламенту, а запит – відповідно до вимог п.6.1 цього Регламенту.

6.5.2. У разі неможливості доступу до власного ключа, підписувач повинен надати до КНЕДП заяву про скасування його чинного сертифікату. У цьому разі отримання нового сертифікату підписувачем здійснюється відповідно до п.6.1.2.

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

6.6.1 Обставини скасування (блокування, поновлення) сертифіката ключа

6.6.1.1 КНЕДП скасовує сертифікат ключа підписувача у разі:

1) подання підписувачем або заявником заяви про скасування виданого йому сертифіката ключа в будь-який спосіб, що забезпечує підтвердження особи-підписувача (заявника);

2) надходження до КНЕДП документа, що підтверджує:

- смерть фізичної особи - підписувача;
- припинення діяльності створювача кваліфікованої електронної печатки;
- зміни ідентифікаційних даних підписувача (заявника);
- факт державної реєстрації припинення підприємницької діяльності фізичної особи - підприємця чи припинення діяльності в установленому законодавством порядку юридичної особи;
- надання заявником недостовірних ідентифікаційних даних під час формування його сертифіката ключа;
- факт компрометації особистого ключа підписувача, виявлений ним самостійно або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;
- набрання законної сили рішенням суду про скасування сертифіката ключа, оголошення підписувача померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності, визнання користувача електронних довірчих послуг банкрутом.

До подій, пов'язаних з компрометацією особистих ключів підписувачів, відносяться наступні:

Будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа, зокрема:

- втрата носіїв, на які записані особисті ключі;
- втрата носіїв, на які записані особисті ключі, з наступним виявленням;
- порушення правил зберігання особистих ключів;
- виникнення підозр на несанкціоноване застосування особистого ключа;
- втрату контролю щодо особистого ключа через компрометацію коду доступу до носія особистого ключа;
- випадки, коли не можна вірогідно встановити, що відбулося з носіями, що містять ключову інформацію (у тому числі, випадки, коли носій вийшов з ладу й доказово не спростована можливість того, що даний факт відбувся в результаті несанкціонованих дій зловмисника).

У випадку компрометації ключа підписувач зобов’язаний терміново сповістити про цей факт КНЕДП та виконати дії згідно пункту 6.6.3 цього Регламенту.

До зміни ідентифікаційних даних підписувача належать:

- переведення на іншу посаду або звільнення з роботи власника сертифіката ключа (для сертифікатів ключів посадових осіб);
- зміна прізвища;
- зміна місця прописки/реєстрації в частині, що вказана в реквізитах власника сертифіката ключа;
- виявлення помилок у реквізитах підписувача, внесених до сертифіката.

6.6.1.2 КНЕДП блокує сертифікат ключа підписувача у разі:

- подання підписувачем (заявником) заяви про блокування виданого йому сертифіката ключа в будь-який спосіб, що забезпечує підтвердження особи-підписувача (заявника);
- повідомлення підписувачем або контролюючим органом про підозру в компрометації особистого ключа підписувача;
- набрання законної сили рішенням суду про блокування сертифіката ключа;
- порушення підписувачем істотних умов договору про надання електронних довірчих послуг.

6.6.1.3 Блокований сертифікат ключа поновлюється у разі:

- подання підписувачем (заявником) заяви про поновлення його заблокованого

сертифіката ключа (якщо блокування здійснено на підставі заяви про блокування сертифіката ключа);

- повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа підписувачем або контролюючим органом, який раніше повідомив про цю підозру;

- надходження до КНЕДП повідомлення про прийняття рішення суду про поновлення сертифіката ключа, що набрало законної сили.

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

Уповноваженими на подання заяви на скасування (блокування, поновлення) сертифіката ключа є підписувачі та заявники.

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

6.6.3.1 Загальні відомості щодо скасування (блокування, поновлення) сертифіката ключа

Блокування тимчасово припиняє дію сертифіката ключа.

Сертифікат ключа, статус якого змінено на заблокований, у період блокування не використовується.

Скасування 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.

6.6.3.2 Порядок блокування сертифіката ключа

Блокування сертифіката здійснюється КНЕДП на підставі заяви, що надходить від підписувача установленим порядком в КНЕДП в усній, паперовій формі чи у вигляді електронного документа або на підставі іншої причини, зазначеної у п. 6.6.1.2 Регламенту.

Сертифікат ключа вважається заблокованим з моменту зміни КНЕДП статусу сертифіката ключа на заблокований.

Блокування сертифіката здійснюється протягом двох годин з моменту настання події, зазначеної у п. 6.6.1.2 Регламенту.

6.6.3.2.1 Блокування сертифіката за заявою в усній формі

Заява на блокування в усній формі подається в КНЕДП за телефоном.

Підписувач повинен повідомити адміністратору реєстрації КНЕДП наступну інформацію:

- ідентифікаційні дані власника сертифікату ключа;

- серійний номер сертифіката, що блокується (якщо підписувач має більш, ніж один діючий сертифікат);

- парольну фразу (слово з парольної фрази) голосової автентифікації.

Заява в усній формі приймається тільки у випадку позитивної автентифікації (збігу даних підписувача та парольної фрази, переданих в заяві, з інформацією, наявною в реєстрі КНЕДП).

Приймання і обробка заяви в усній формі здійснюється цілодобово. Обробка заяви в усній формі на блокування сертифіката та інформування підписувача здійснюється безпосередньо після приймання заяви протягом двох годин.

6.6.3.2.2 Блокування сертифіката за заявою в паперовій формі

Заява в паперовій формі подається в КНЕДП за встановленою формою, яку можливо отримати з електронного інформаційного ресурсу КНЕДП.

Заява на блокування сертифіката засвідчується відповідно до п. 5.7 Регламенту.

Подача заяви на блокування сертифіката в КНЕДП та її розгляд здійснюється тільки в робочий час, відповідно до розпорядку роботи КНЕДП.

6.6.3.2.3 Блокування сертифіката за заявою у електронній формі

Електронна заява подається до КНЕДП за встановленою формою та засвідчується підписувачем за допомогою свого особистого ключа (якщо відповідний сертифікат ключа є чинним) і кваліфікованою електронною печаткою організації (в разі наявності).

Подача заяви на блокування сертифіката в КНЕДП та її розгляд здійснюється цілодобово в режимі реального часу за допомогою відповідного модулю ПТК КНЕДП.

6.6.3.3 Порядок скасування сертифіката ключа

6.6.3.3.1 Скасування сертифіката здійснюється КНЕДП на підставі заяви, що надходить від підписувача установленим порядком в КНЕДП в паперовій формі чи у вигляді електронного документа або на підставі іншої причини, зазначеної у п. 6.6.1.1 Регламенту.

6.6.3.3.2. Заява на скасування сертифіката в паперовій формі подається в КНЕДП за відповідною формою, яка доступна на інформаційному ресурсі КНЕДП.

Заява на скасування сертифіката засвідчується відповідно до п. 5.7 Регламенту.

Подача заяви на скасування сертифіката в КНЕДП та її розгляд здійснюється тільки в робочий час, відповідно до розпорядку роботи КНЕДП.

6.6.3.3.3. Електронна заява подається до КНЕДП за встановленою формою та засвідчується підписувачем (заявником) за допомогою свого особистого ключа (якщо відповідний сертифікат ключа є чинним) і кваліфікованою електронною печаткою організації (в разі наявності).

Подача заяви на скасування сертифіката в КНЕДП та її розгляд здійснюється цілодобово в режимі реального часу за допомогою відповідного модулю ПТК КНЕДП.

6.6.3.3.4. 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.

6.6.3.3.5. Скасування сертифіката здійснюється протягом двох годин з моменту настання події, зазначеної у п. 6.6.1.1 Регламенту.

Сертифікат ключа вважається скасованим з моменту зміни КНЕДП статусу сертифіката ключа на скасований.

6.6.3.4 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 КНЕДП на підставі заяви, що надходить встановленим порядком в КНЕДП в паперовій формі.

Заява на поновлення сертифіката подається в КНЕДП за відповідною формою, яка доступна на інформаційному ресурсі КНЕДП.

Подача заяви на поновлення чинності сертифіката в КНЕДП та її розгляд здійснюється тільки в робочий час, відповідно до розпорядку роботи КНЕДП.

Поновлення сертифіката здійснюється протягом двох годин з моменту настання події, зазначеної у п. 6.6.1.3 Регламенту.

Сертифікат ключа вважається поновленим з моменту зміни КНЕДП статусу сертифіката ключа на чинний.

6.6.4. Порядок та умови блокування, поновлення, скасування сертифікатів ключів підписувачів, які є працівниками Банку, визначаються внутрішнім розпорядчим документом Банку.

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

6.7.1 Частота формування списку відкликаних сертифікатів та строки його дії

Публікація списків відкликаних сертифікатів на електронному інформаційному ресурсі КНЕДП здійснюється у порядку, визначеному у п. 5.3.3 цього Регламенту.

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.

6.8 Строки дії сертифікатів ключів, сформованих КНЕДП

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 КНЕДП – не більше ніж 2 роки;
- сертифікат ключа підписувача – не більше ніж 2 роки.

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

7.1 Надання засобів кваліфікованого електронного підпису чи печатки

КНЕДП для надання кваліфікованих електронних довірчих послуг використовуються засоби кваліфікованого електронного підпису чи печатки, які мають позитивний експертний висновок за результатами їх державної експертизи у сфері КЗІ.

Надання КНЕДП клієнтам Банку засобів кваліфікованого 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 КНЕДП засобів кваліфікованого електронного підпису чи печатки може здійснюватися шляхом надання доступу до відповідних сервісів через офіційний електронний інформаційний ресурс КНЕДП.

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 позитивної двофакторної автентифікації, делегує застосування свого особистого ключа КНЕДП для створення кваліфікованого електронного підпису та/або розшифрування та/або автентифікації.

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

Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження кваліфікованої електронної позначки часу надається підписувачам та створювачам електронних печаток.

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

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

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

7.3 Необхідні вимоги до процедур

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

Зазначені вимоги затверджуються як окремий документ КНЕДП.