**Затверджую**
Керівник Центру сертифікації ключів
АТ «Укрексімбанк»
Березко О.Ю.
«22» 2015 року

**Погоджую**
Заступник Голови
Національного банку України
Смолій Я.В.
«__» 2015 року

**Регламент роботи Центра сертифікації ключів АТ «Укрексімбанк»**

**Зміст**

## 1. Загальні положення.

1.1. Цей Регламент роботи Центра сертифікації ключів АТ «Укрексімбанк» (далі - Регламент) розроблено відповідно до Регламенту роботи Засвідчувального центру Національного банку України, правил розроблення Регламенту роботи центрів сертифікації ключів банків України, інших нормативно-правових актів Національного банку України з питань застосування електронного цифрового підпису.

1.2. У Регламенті скорочення вживаються в такому значенні:

**БД** - база даних;
**заявник** - заявник підписувача, який є клієнтом банку;
**ЕЦП** - електронний цифровий підпис;
**НКІ** - носій ключової інформації;
**ЗЦ НБУ** - Засвідчувальний центр Національного банку України;
**ПЗ** - програмне забезпечення;
**ПТК** - програмно-технічний комплекс;
**сертифікат ключа** – сертифікат відкритого ключа;
**СВС** - список відкликаних сертифікатів ключів;
**СЗІ** - система захисту інформації;
**ЦСК** - центр сертифікації ключів АТ «Укрексімбанк»;
**DNS** - доменна система іменування;
**HTTP** - протокол прикладного рівня, що використовується для передавання гіпертексту;
**IMAP4** - протокол інтерактивного доступу до електронної пошти;
**LDAP** - полегшений (спрощений) протокол доступу до каталогів;
**NTP** - протокол мережного часу;
**OCSP** - протокол визначення статусу сертифіката ключа;
**POP3** - поштовий протокол версії 3;
**SMTP** - простий протокол передавання електронної пошти;
**TCP** - протокол керування передаванням;
**TSP** - протокол фіксування часу.

Інші скорочення в цьому Регламенті застосовуються в значеннях, наведених у документах, зазначених у пункті 1.1 цього Регламенту.

1.3. У цьому Регламенті терміни вживаються в такому значенні:

**БД** - база даних ЦСК, у якій зберігаються реєстр ЦСК, інформаційно-довідкова, технологічна та інша службова інформація, потрібна для функціонування ПТК ЦСК;

**договір, відповідно до якого підписувачу надаються послуги ЕЦП,** - окремий договір про надання послуг ЕЦП або договір про обслуговування клієнта банку чи додаток до нього, що має містити договір про надання послуг ЕЦП підписувачу. Підписувачі, які є працівниками банку, не укладають з ЦСК договір про надання послуг ЕЦП;

**заявник** – підписувач який є клієнтом банку або уповноважений представник підписувача, який є клієнтом банку, у ЦСК, який на законних підставах звертається до ЦСК з метою організації та проведення процедури реєстрації підписувача - клієнта банку формування та зміни статусу його сертифіката ключа, а також зміни його даних (реквізитів) у встановленому порядку. Якщо в основних даних (реквізитах) сертифіката 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 ключа підписувача, які попередньо надавалися заявником до ЦСК;

**зміна статусу сертифіката ключа** - виконання однієї з процедур блокування/скасування/поновлення сертифіката ключа;

**інформаційний ресурс ЦСК** - загальнодоступна інформація про ЦСК. Доступ до інформаційного ресурсу ЦСК є вільним і забезпечується через телекомунікаційні мережі загального користування;

**СЗІ ПТК ЦСК** - сукупність інженерно-технічних, організаційних заходів і програмно-апаратних засобів, що забезпечують технічний та криптографічний захист інформації в ПТК ЦСК;

**підписувач, який є клієнтом банку,** - клієнт банку, якому ЦСК надає послуги ЕЦП. Банк укладає з підписувачем - клієнтом банку договір, відповідно до якого підписувачу надаються послуги ЕЦП;

**підписувач, який є працівником** банку, - працівник банку, який для виконання своїх службових обов'язків користується послугами ЕЦП ЦСК. Банк призначає підписувача - працівника банку наказом або службовим розпорядженням;

**поновлення сертифіката ключа** - процедура управління статусом сертифіката ключа, що поновлює чинність сертифіката ключа (якій передувала відповідна процедура блокування сертифіката ключа);

**ПТК ЦСК** - сукупність технічного обладнання та ПЗ, що використовуються банком, у якому функціонує ЦСК, для забезпечення виконання функцій ЦСК;

**процедура реєстрації підписувача, який є клієнтом банку,** - установлена процедура подання заявником до ЦСК необхідного пакета документів, опрацювання цих документів і формування сертифіката ключа підписувача - клієнта банку;

**процедура реєстрації підписувача, який є працівником банку,** - установлена процедура подання ним до ЦСК необхідного пакета документів, опрацювання цих документів і формування сертифіката ключа підписувача - працівника банку;

**реєстр ЦСК** – реєстр у ЦСК з унесеними до нього сертифікатами відкритих ключів самого ЦСК, відповідальних осіб ЦСК та підписувачів (у тому числі блокованими і скасованими) і даними про ЦСК, відповідальних осіб ЦСК та підписувачів;

**сертифікат ключа відповідальної особи ЦСК** - сертифікат ключа відповідальної особи ЦСК, чинність якого засвідчується особистими ключами ЦСК;

**скасування сертифіката ключа** - процедура управління статусом сертифіката ключа, яка зупиняє чинність сертифіката ключа;

**строк чинності сертифіката ключа** - проміжок часу між датою і часом початку та датою і часом закінчення чинності сертифіката ключа, що встановлюються під час формування сертифіката ключа;

**строк чинності особистого ключа** - строк, протягом якого використання особистого ключа є чинним. Строк чинності особистого ключа визначається строком чинності сертифікату ключа для відповідного публічного ключа.

Інші терміни в цьому Регламенті застосовуються в значеннях, наведених у Законі України "Про електронний цифровий підпис" і документах, зазначених у пункті 1.1 цього Регламенту.

1.4. Цей Регламент є внутрішнім документом банку, що визначає організаційно-методологічні та технологічні умови діяльності ЦСК під час реєстрації, зміни ідентифікаційних даних підписувачів і надання підписувачам послуг ЕЦП.

1.5. Положення цього Регламенту поширюються в електронній формі шляхом розміщення на інформаційному ресурсі ЦСК.

1.6. Суб'єктами правових відносин у сфері ЕЦП, що обумовлюються цим Регламентом, є ЗЦ НБУ, ЦСК і підписувачі.

1.7. Вимоги цього Регламенту поширюються на всі причетні сторони, а також є засобом офіційного повідомлення та інформування всіх сторін у взаєминах, що виникають у процесі надання і використання послуг ЕЦП від ЦСК.

1.8. Ідентифікаційні дані ЦСК:

- повне найменування банку: **Публічне акціонерне товариство «Державний експортно-імпортний банк України»**;
- повне найменування ЦСК: **Центр сертифікації ключів АТ «Укрексімбанк»**;
- ідентифікаційний код юридичної особи (банку): **00032112**;
- адреса розташування ЦСК: **Україна, 03150, м. Київ, вул. Горького, 127**;
- телефони ЦСК: **(044) 247-80-28**, **(044) 247-89-41**;
- факс ЦСК: **(044) 247-80-82**;
- електронна адреса інформаційного ресурсу ЦСК (веб-сайта): **https://www.eximb.com/ukr/corporate/internet_banking/safety/ca**,

  **https://www.eximb.com/ukr/sme/everyday/internet_banking/safety/ca**;
- електронна поштова скринька ЦСК: **ca@hq.eximb.com**.

## 2. Організаційна структура ЦСК

2.1. Організаційна структура ЦСК містить дві основні складові частини, що виконують адміністративні функції, технічні і технологічні функції.

2.2. До адміністративних функцій ЦСК належать:

- реєстрація підписувачів;
- надання підписувачам консультацій з питань, пов'язаних з використанням ЕЦП;
- розгляд заяв і скарг підписувачів;
- передавання документованої інформації, яка підлягає обов'язковому передаванню в разі припинення діяльності ЦСК, до ЗЦ НБУ.

2.3. До технічних і технологічних функцій ЦСК належать:

- створення і забезпечення функціонування ПТК ЦСК;
- забезпечення захисту інформації впродовж експлуатації ПТК ЦСК;
- генерування і зберігання ключів ЦСК та відповідальних осіб ЦСК;
- 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;
- засвідчення чинності власних відкритих ключів ЦСК у ЗЦ НБУ;
- формування сертифікатів ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб ЦСК і підписувачів;
- ведення реєстру ЦСК;
- поширення сертифікатів ключів ЦСК і підписувачів у встановленому цим Регламентом порядку;
- блокування, скасування та поновлення сертифікатів ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб ЦСК і

підписувачів у випадках, передбачених цим Регламентом і законодавством України у сфері ЕЦП;

- надання підписувачам послуг фіксування часу;
- надання послуг визначення статусу сертифіката ключа;
- публікація на інформаційному ресурсі ЦСК відкритої інформації;
- інші дії, пов'язані з технічною та технологічною підтримкою діяльності ЦСК.

2.4. У ЦСК для виконання адміністративних, технічних і технологічних функцій створено такі служби:

- служба захисту інформації;
- служба сертифікації;
- служба реєстрації;
- служба системного адміністрування.

2.5. Основними функціями служби захисту інформації є:

- проектування, розроблення, експлуатація, обслуговування та модернізація СЗІ ПТК ЦСК;
- адміністрування відповідальних осіб ЦСК.

2.6. Основними функціями служби сертифікації є:

- генерування ключів ЦСК;
- вивантаження з ПТК ЦСК власних відкритих ключів ЦСК для засвідчення їх чинності в ЗЦ НБУ;
- завантаження сертифікатів власних ключів ЦСК в ПТК ЦСК;
- перехід на використання нових ключів ЦСК;
- знищення особистих ключів ЦСК, строк чинності яких закінчився;
- засвідчення чинності відкритих ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб ЦСК і підписувачів;
- звернення до ЗЦ НБУ щодо зміни статусу власних сертифікатів ключів ЦСК у випадках, передбачених цим Регламентом і законодавством України у сфері ЕЦП;
- управління статусом сертифікатів ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб ЦСК і підписувачів;
- надання підписувачам послуг фіксування часу;
- надання послуг визначення статусу сертифікатів ключів ЦСК і підписувачів користувачам послуг ЕЦП;
- надання відповідальним особам ЦСК послуг визначення статусу сертифікатів ключів відповідальних осіб ЦСК;
- вивантаження/завантаження резервної інформації із/в ПТК ЦСК.
- унесення змін до реєстру ЦСК щодо статусу підписувачів.

2.7. Основними функціями служби реєстрації є:

- опрацювання документів, які подаються заявником до ЦСК під час проведення процедур реєстрації, формування сертифікатів ключів, зміни статусу сертифікатів ключів, зміни ідентифікаційних даних підписувача, який є клієнтом банку, чи припинення дії/зміни договору, відповідно до якого цьому підписувачу - клієнту банку надаються послуги ЕЦП;
- опрацювання документів, які подаються підписувачем - працівником банку під час проведення процедур реєстрації, формування сертифікатів ключів, зміни статусу сертифікатів ключів, зміни його ідентифікаційних даних;
- надання допомоги під час генерування ключів підписувачів у разі потреби та вживання заходів щодо забезпечення безпеки інформації під час генерування ключів;
- уведення чи генерування в ПТК ЦСК запитів на формування сертифікатів ключів підписувачів для виконання засвідчення їх чинності;
- генерування в ПТК ЦСК запитів на блокування, скасування чи поновлення сертифікатів ключів під час подання відповідних заяв;
- розгляд скарг підписувачів;

2.8. Основними функціями служби адміністрування є:

- установлення та налаштування серверних застосувань в ПТК ЦСК;
- виконання оновлень ПЗ ПТК ЦСК;
- підтримка належного функціонування ПТК ЦСК.

2.9. Відповідальні особи ЦСК виконують роботу з нормативно-довідковою інформацією ЦСК згідно з Політикою інформаційної безпеки Банку і наданих їм адміністратором безпеки ЦСК повноважень.

2.10. Служба реєстрації ЦСК надає доступ до неспеціалізованого робочого місця для генерування ключів підписувачу, який є працівником банку, чи забезпечує їх генерування на робочому місці підписувача - працівника банку згідно з Політикою інформаційної безпеки банку.

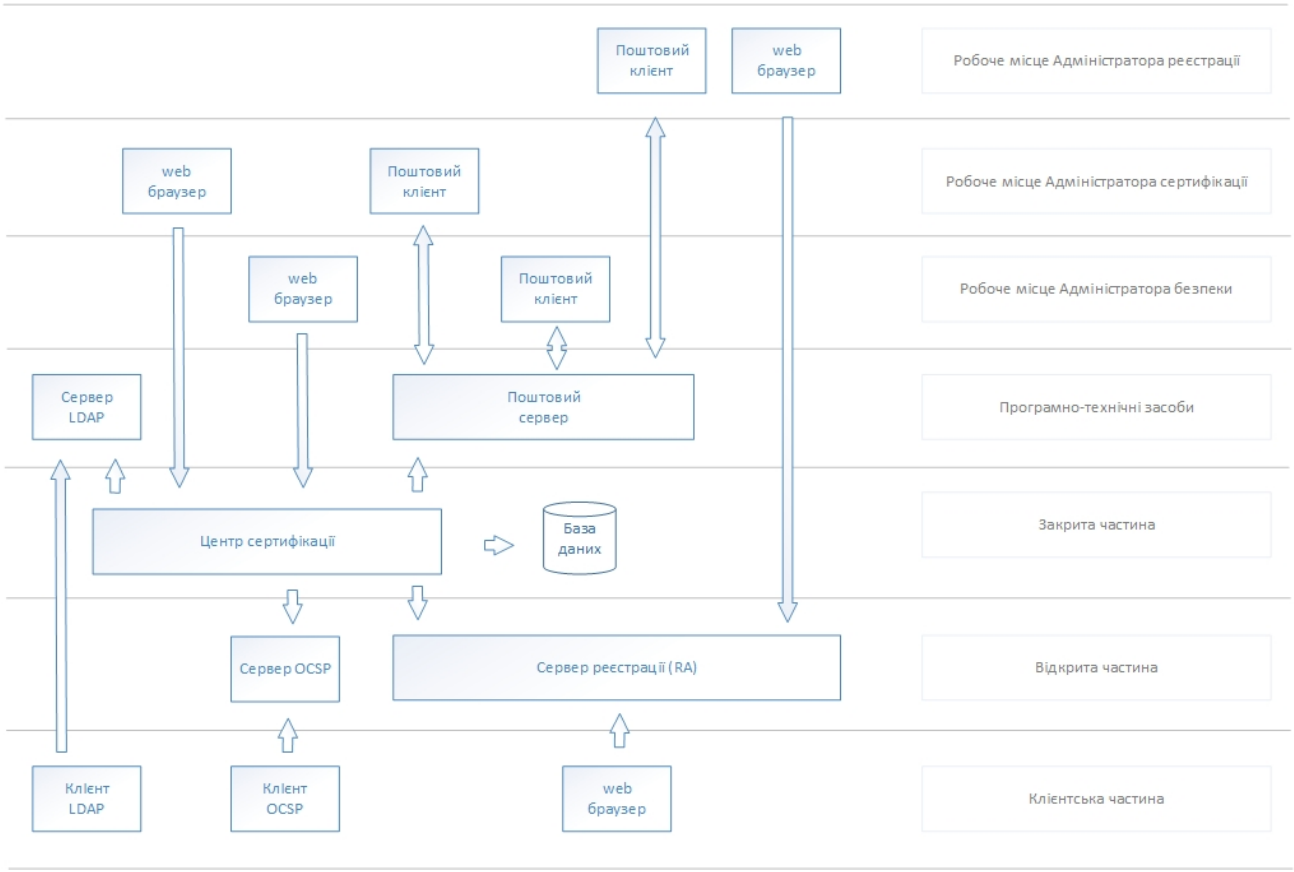
2.11. Служба реєстрації ЦСК надає доступ до неспеціалізованого робочого місця заявнику для генерування ключів підписувача, який є клієнтом банку, у разі потреби згідно з Політикою інформаційної безпеки банку.

2.12. Відповідальні особи ЦСК не можуть суміщати функції служби захисту інформації ЦСК з функціями інших служб ЦСК.

2.13. Усі відповідальні особи ЦСК перед початком виконання своїх функціональних обов'язків повинні ознайомитися зі змістом цього Регламенту, інструкцій щодо роботи в ПТК ЦСК, інструкції щодо забезпечення безпеки експлуатації засобів криптографічного захисту інформації та порядку генерування ключових даних і поводження з ключовими документами, Політиками інформаційної безпеки Банку. Відповідальні особи ЦСК підтверджують факт ознайомлення з цими документами під підпис.

2.14. ЦСК створює відокремлені пункти реєстрації у філіях банку для ефективного надання послуг ЕЦП. Відокремлені пункти реєстрації виконують функції служби реєстрації ЦСК.

## 3. Архітектура ПТК ЦСК




3.1. Технічні засоби комплексу об'єднані в розподілену обчислювальну мережу з використанням телекомунікаційної мережі банку, частина засобів підключена до загальнодоступних телекомунікаційних мереж.

3.2. Апаратне комп'ютерне забезпечення ПТК ЦСК складається з двох типів комп'ютерної техніки, а саме:

- серверної комп'ютерної техніки;
- клієнтської комп'ютерної техніки.

3.3. ПЗ ПТК ЦСК є централізованим трирівневим комплексом, що складається з таких компонентів:

- БД;
- серверних застосувань;
- клієнтських застосувань.

3.4. БД, клієнтське застосування системи керування БД та серверні застосування розташовані на серверній комп'ютерній техніці.

3.5. Усі інші клієнтські застосування, що використовуються в ПТК ЦСК, розташовані на клієнтській комп'ютерній техніці (на робочих місцях відповідальних осіб ЦСК).

3.6. У ПТК ЦСК організовано основні та резервні робочі місця адміністратора безпеки ЦСК та адміністратора сертифікації ЦСК.

3.7. Серверні застосування виконують такі технічні і технологічні функції ПТК ЦСК:

- завантаження/вивантаження інформації в/із БД;
- формування сертифікатів ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб ЦСК і підписувачів;
- поширення сертифікатів ключів ЦСК і підписувачів;
- блокування, скасування та поновлення сертифікатів ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб ЦСК і підписувачів;
- формування СВС;
- надання підписувачам послуг фіксування часу;
- надання послуг визначення статусу сертифіката ключа;
- зберігання та поширення нормативно-довідкової інформації ЦСК;
- ідентифікація, автентифікація та авторизація відповідальних осіб ЦСК;
- забезпечення синхронізації часу ПТК ЦСК із всесвітнім координованим часом (UTC) згідно Процедури синхронізації часу АТ «Укрексімбанк».

3.8. Клієнтські застосування ініціюють виконання:

- технічних і технологічних функцій серверними застосуваннями;
- генерування ключів ЦСК та відповідальних осіб ЦСК за допомогою надійних засобів ЕЦП;
- генерування ключів підписувачів за допомогою засобів ЕЦП;
- вивантаження із ПТК ЦСК власних відкритих ключів ЦСК для засвідчення їх чинності в ЗЦ НБУ.

3.9. Лише серверні застосування можуть виконувати завантаження/вивантаження інформації в/із БД шляхом використання клієнтського застосування системи керування БД. Клієнтські застосування, розташовані на робочих місцях, отримують доступ до інформації в БД за допомогою серверних застосувань.

3.10. Відповідальні особи ЦСК здійснюють генерування і використання ключів відповідно до своїх функціональних обов'язків виключно на своїх робочих місцях.

3.11. Серверна комп'ютерна техніка ПТК ЦСК складається з трьох серверів і має кластерну архітектуру. Інформація циркулює між серверами за допомогою мережі збереження даних.

3.12. Кластерне рішення в штатному режимі роботи забезпечує функціонування БД, клієнтського застосування системи керування БД та серверних застосувань на одному із серверів. Кластерне рішення автоматично переводить роботу зазначеного ПЗ на інший сервер кластеру без виникнення простоїв у роботі та втрати інформації під час виникнення проблем у роботі.

## 4. Режими доступу до інформації в ЦСК

4.1. У ЦСК циркулює інформація, яка за режимом доступу поділяється на відкриту інформацію та інформацію з обмеженим доступом.

4.2. До відкритої інформації ЦСК належать:

- зміст цього Регламенту;

- нормативні документи та нормативно-довідкові матеріали;
- сертифікати ключів ЦСК, відповідальних осіб ЦСК і підписувачів;
- інформація про статус сертифікатів ключів ЦСК, відповідальних осіб ЦСК і підписувачів.

4.3. До інформації з обмеженим доступом ЦСК в електронній формі належать:

- особисті ключі ЦСК і відповідальних осіб ЦСК;
- інформація про підписувачів, що міститься в ЦСК і не підлягає безпосередньому поширенню як частина сертифіката ключа;
- налаштування технічних і програмних засобів ПТК ЦСК;
- зміст протоколів роботи ПТК ЦСК.

4.4. До інформації з обмеженим доступом ЦСК на паперових носіях належать документи, що подаються до ЦСК під час проведення процедур реєстрації, формування сертифікатів ключів, зміни статусу сертифікатів ключів, зміни ідентифікаційних даних підписувачів і не підлягають безпосередньому оприлюдненню.

4.5. Відкрита інформація може опубліковуватися на інформаційному ресурсі ЦСК.

4.6. Доступ до інформації з обмеженим доступом, що циркулює в ЦСК, мають відповідальні особи ЦСК згідно з Політикою інформаційної безпеки Банку.

4.7. ЦСК має право надавати доступ до інформації з обмеженим доступом іншим особам лише у випадках, передбачених законодавством України.

## 5. Захист інформації в ПТК ЦСК

5.1. Захист інформації в ПТК ЦСК забезпечується в результаті впровадження СЗІ.

5.2. СЗІ ПТК ЦСК відповідає вимогам нормативно-правових актів Національного банку України з питань захисту інформації.

5.3. У ПТК ЦСК використовуються такі захищені НКІ:

- USB токени;
- Модулі безпеки (HSM).

5.4. На захищених НКІ, а саме в модулях безпеки (HSM), з власними ключами ЦСК та послуги інтерактивного визначення статусу сертифіката містяться такі дані:

- поточний та майбутній (у разі наявності) власні особисті ключі ЦСК;
- поточний сертифікат власного відкритого ключа ЦСК і майбутній відкритий ключ (у разі наявності).

5.5. На захищених НКІ відповідальних осіб ЦСК і підписувачів містяться такі дані:

- поточний та майбутній (у разі наявності) особисті ключі відповідальних осіб ЦСК;
- поточний сертифікат ключа та майбутній відкритий ключ (у разі наявності).

5.6. Серверна комп'ютерна техніка ПТК ЦСК розміщується в серверних приміщеннях або в спеціалізованих приміщеннях з обмеженим доступом обладнаних системою санкціонованого доступу та охоронною системою виведеною на центральний пульт, подвійну системою кондиціонування з виведенням на центральний пульт, незалежною системою оповіщення температурного режиму приміщення каналом мобільного зв‘язку.

5.7. Серверні приміщення та приміщення з обмеженим доступом відповідають вимогам Правил з технічного захисту інформації для комутаційних кімнат, серверних приміщень, приміщень електронних архівів, екранованих та спеціалізованих приміщень АТ «Укрексімбанк».

5.8. Генерування ключів ЦСК виконується адміністратором сертифікації ЦСК лише у присутності адміністратора безпеки ЦСК.

5.9. Відповідальні особи ЦСК повинні зберігати НКІ зі своїми криптографічними ключами у сейфах/ящиках/шафах, що надійно замикаються і до яких не мають доступу сторонні особи і несуть особисту відповідальність за надійне зберігання НКІ та нерозголошення значення паролів доступу і розблокування.

5.10. Серверні застосування забезпечують можливість:

- криптографічного захисту інформації, що передається каналами зв'язку (автентифікація та шифрування);
- захищеного від модифікації протоколювання подій, визначених цим Регламентом;
- використання засобів антивірусного захисту на комп'ютерах ПТК ЦСК.

5.11. Захист персональних даних підписувачів забезпечується шляхом ужиття:

- організаційних заходів щодо обліку та зберігання справ підписувачів, зокрема, формування справ підписувачів та їх облік, призначення осіб, відповідальних за зберігання справ підписувачів, обмежений доступ до приміщень (шаф), де зберігаються справи підписувачів;
- організаційно-технічних і технічних заходів, реалізованих у результаті впровадження СЗІ, у тому числі: використання антивірусних засобів, міжмережевих екранів тощо.

## 6. Журнали аудиту в ПТК ЦСК

6.1. У ПТК ЦСК ведуться такі журнали аудиту:

- журнали функціонування ПЗ в ПТК ЦСК;
- журнал технічного обслуговування ПТК ЦСК.

6.2. Журнали функціонування ПЗ в ПТК ЦСК ведуться в електронній формі на всіх серверних застосуваннях. Інші журнали ведуться на паперових носіях.

6.3. ПЗ ПТК ЦСК забезпечує захищене від модифікації протоколювання подій, пов'язаних з функціонуванням ПЗ. Захист від модифікації забезпечується встановленням правил розмежування доступу засобами операційної системи та обчисленням контрольних сум для записів у журналі. Цей журнал подій містить дату та час події, опис події. У журналі реєструються події, пов'язані з:

- формуванням, переформуванням, зміною статусу сертифікатів ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб ЦСК і підписувачів;
- унесенням, модифікацією та видаленням даних про послуги інтерактивного визначення статусу сертифіката, відповідальних осіб ЦСК і підписувачів.

6.4. Системний адміністратор веде журнал регламентних робіт з технічного обслуговування ПТК ЦСК. Цей журнал містить дату та час події, її опис. У журналі реєструються події, пов'язані з:

- плановою заміною комп'ютерної техніки ПТК ЦСК;

- виходом з ладу складових комп'ютерної техніки ПТК ЦСК та їх ремонтом/заміною;
- встановленням та оновленням ПЗ ЦСК.

6.5. Відповідальні особи ЦСК, які ведуть журнали аудиту, зберігають їх у сейфах або в шафах, що надійно замикаються і до яких не мають доступу сторонні особи.

6.6. Копії електронних журналів функціонування ПЗ в ПТК ЦСК автоматично в режимі он-лайн копіюються до системи реєстрації та зберігання подій безпеки банку.

6.7. Відповідальні особи ЦСК переглядають журнали аудиту в ПТК ЦСК у разі потреби.

6.8. Адміністратор служби захисту інформації ЦСК забезпечує за зверненням відповідальних осіб ЦСК перегляд журналів аудиту, що ведуться:

- серверними застосуваннями;
- іншими відповідальними особами ЦСК.

6.9. Строк зберігання журналів аудиту в ПТК ЦСК становить п'ять років.

## 7. Особисті ключі в ЦСК

7.1. Відповідальні особи ЦСК, які здійснюють генерування ключів, що використовуються в ЦСК, застосовують виключно захищені пристрої НКІ.

7.2. Особисті ключі, що використовуються в ЦСК, зберігаються виключно всередині захищених пристроїв НКІ.

7.3. Строк чинності особистого ключа дорівнює строку чинності відповідного сертифіката ключа. Особистий ключ тимчасово не є чинним у разі блокування відповідного сертифіката ключа.

7.4. У ЦСК генеруються та використовуються такі криптографічні ключі:

- власні (особистий та відкритий) ключі ЦСК для криптографічного алгоритму RSA (довжина 2048 біт);
- особистий та відкритий ключі послуги фіксування часу ЦСК для криптографічного алгоритму RSA (довжина 2048 біт);
- особистий та відкритий ключі ЦСК послуги визначення статусу сертифіката для криптографічного алгоритму RSA (довжина 2048 біт);
- особистий та відкритий ключі відповідальних осіб ЦСК для криптографічного алгоритму RSA (довжина 2048 біт);

7.5. Служба реєстрації ЦСК забезпечує підписувача засобами ЕЦП та надає йому допомогу під час генерування ключів у разі потреби.

7.6. Власні особисті ключі ЦСК використовуються виключно для формування СВС, сертифікатів ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб ЦСК та підписувачів.

7.7. Особисті ключі ЦСК послуги фіксування часу використовуються виключно під час формування відповіді на запит на позначку часу.

7.8. Особисті ключі ЦСК послуги визначення статусу сертифіката використовуються виключно під час формування відповіді на запит про статус сертифіката.

7.9. Особисті ключі відповідальних осіб ЦСК використовуються виключно для їх автентифікації в ПТК ЦСК.

7.10. Особистий ключ підписувача, що відповідає відкритому ключу, сертифікат якого сформовано в ЦСК, використовується відповідно до переліку сфер використання сертифіката, основних обмежень та інших даних, включених до сертифіката ключа підписувача на його вимогу.

7.11. Адміністратор сертифікації ЦСК відповідає за виконання процедур генерування та резервування ключів ЦСК. Адміністратор сертифікації ЦСК здійснює ці процедури на своєму робочому місці під контролем адміністратора безпеки ЦСК. Резервування виконується тільки під час генерування ключів ЦСК на кількох носіях засобами захищених НКІ.

7.12. Відповідальні особи ЦСК самостійно виконують генерування ключів, які використовуються для виконання їх функціональних обов'язків, на свої робочих місцях.

7.13. Служба сертифікації ЦСК самостійно приймає рішення про факт або загрозу компрометації особистих ключів ЦСК чи пароля доступу до пристроїв НКІ, на яких вони записані.

7.14. Служба сертифікації ЦСК у разі компрометації або загрози компрометації власних особистих ключів ЦСК:

- подає заяву про скасування (або блокування та подальше скасування) сертифікатів власних ключів ЦСК у ЗЦ НБУ;
- знищує поточні основні та всі резервні копії власних особистих ключів ЦСК методом, що не допускає можливості їх відновлення (після скасування в ЗЦ НБУ поточних сертифікатів ключів ЦСК);
- виконує генерування нових власних ключів ЦСК;
- засвідчує власні відкриті ключі ЦСК у ЗЦ НБУ;
- переходить на використання нових власних ключів ЦСК.

7.15. Служба сертифікації ЦСК у разі компрометації або загрози компрометації особистих ключів послуги інтерактивного визначення статусу сертифіката:

- скасовує (або блокує з подальшим скасуванням) сертифікати цієї послуги ЦСК;
- знищує поточні основні та всі резервні копії особистих ключів цієї послуги ЦСК методом, що не допускає можливості їх відновлення;
- виконує генерування нових ключів для цієї послуги ЦСК;
- формує сертифікати ключів цієї послуги ЦСК;
- переходить на використання нових ключів цієї послуги ЦСК.

7.16. Відповідальна особа ЦСК самостійно приймає рішення про факт або загрозу компрометації свого особистого ключа чи пароля доступу до НКІ.

7.17. Відповідальна особа ЦСК формує новий сертифікат ключа у визначеному цим Регламентом порядку в разі компрометації чи загрози компрометації особистого ключа.

7.18. Відповідальна особа ЦСК негайно змінює пароль доступу до НКІ в разі компрометації чи загрози компрометації пароля доступу.

7.19. Служба сертифікації ЦСК знищує основні та всі резервні копії особистих ключів ЦСК після закінчення їх строку чинності методом, що не допускає можливості їх відновлення.

7.20. Відповідальні особи ЦСК знищують свої особисті ключі після закінчення їх строку чинності методом, що не допускає можливості їх відновлення.

## 8. Сертифікати ключів у ЦСК

8.1. Сертифікати ключів ЦСК, відповідальних осіб ЦСК та підписувачів зберігаються в реєстрі ЦСК.

8.2. СВС та сертифікати ключів ЦСК, відповідальних осіб ЦСК і підписувачів формуються ЦСК відповідно до формату X.509 v3 з урахуванням вимог стандарту ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

8.3. ЗЦ НБУ формує сертифікати власних ключів ЦСК та сертифікати ключів ЦСК для послуги фіксування часу.

8.4. Служба сертифікації ЦСК формує сертифікати ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб ЦСК та підписувачів.

8.5. Сертифікати власних ключів ЦСК використовуються виключно для перевірки СВС, сертифікатів ключів послуги інтерактивного визначення статусу сертифіката, відповідальних осіб ЦСК та підписувачів.

8.6. Сертифікати ключів послуги інтерактивного визначення статусу сертифіката використовуються виключно для перевірки ЕЦП під час визначення статусу сертифікатів ключів.

8.7. Сертифікати ключів послуги послуг фіксування часу використовуються виключно для перевірки ЕЦП на позначці часу під час надання послуг фіксування часу.

8.8. Сертифікати ключів відповідальних осіб ЦСК використовуються виключно для ідентифікації та автентифікації відповідальних осіб ЦСК під час роботи в ПТК ЦСК та перевірки ЕЦП.

8.9. ЦСК під час формування сертифікатів ключів підписувачів зазначає сфери використання цих сертифікатів та обмеження щодо їх використання.

8.10. Строк чинності сертифікатів ключів ЦСК становить два роки після чого проводиться їх планова заміна згідно з вимогами цього Регламенту.

8.11. Строк чинності сертифікатів ключів відповідальних осіб ЦСК становить два роки після чого проводиться їх планова заміна згідно з вимогами цього Регламенту.

8.12. Строк чинності сертифікатів ключів підписувачів становить один рік після чого проводиться їх планова заміна згідно з вимогами цього Регламенту.

8.13. Строк чинності сертифіката ключа закінчується в разі його скасування. Сертифікат ключа тимчасово не є чинним протягом строку його блокування.

8.14. Сертифікати відповідальних осіб ЦСК зберігаються виключно на НКІ та в БД ПТК ЦСК.

## 9. Порядок подання документів під час проведення регламентних процедур

9.1. Подання документів для проведення регламентних процедур в ЦСК при роботі з заявником/підписувачем, який є клієнтом банку, виконується під час укладання Договору на обслуговування у системі Enter EXIM® та регламентується Інструкцією про порядок відкриття, використання і закриття рахунків у національній та іноземних валютах затвердженою Постановою Правління Національного банку України від 12.11.2003 року №492.

9.2. Подання документів для проведення регламентних процедур в ЦСК при роботі з підписувачем, який є працівником банку регламентується внутрішніми документами Банку.

## 10. Порядок опрацювання документів, що подаються до ЦСК під час проведення регламентних процедур

10.1. Опрацювання документів, що подаються до ЦСК під час проведення регламентних процедур при роботі з заявником/підписувачем, який є клієнтом банку, виконується під час укладання Договору на обслуговування у системі Enter EXIM® та регламентується Інструкцією про порядок відкриття, використання і закриття рахунків у національній та іноземних валютах затвердженою Постановою Правління Національного банку України від 12.11.2003 року №492.

10.2. Опрацювання документів, що подаються до ЦСК під час проведення регламентних процедур при роботі з підписувачем, який є працівником банку регламентується внутрішніми документами Банку.

## 11. Реєстрація підписувачів

11.1. Реєстрація підписувачів регламентується внутрішніми документами Банку.

11.2. Підписувач перед початком процедури реєстрації повинен ознайомитися з умовами обслуговування сертифікатів ключів, щодо:

- зобов'язань та підстав відповідальності ЦСК стосовно обслуговування сертифікатів ключів;
- зобов'язань та підстав відповідальності підписувача стосовно використання сертифіката ключа і зберігання особистого ключа;
- сфери використання підписувачем сертифіката ключа;
- строків зберігання в ЦСК даних про підписувачів, що були отримані ЦСК під час реєстрації.
- відомостей про засоби ЕЦП, що можуть використовуватися для формування та перевірки ЕЦП. Підписувач, який є працівником банку, для проведення реєстрації підписує зобов'язання про дотримання умов використання ЕЦП.

11.3. ЦСК здійснює скасування реєстрації підписувача в такому порядку:

- служба реєстрації ЦСК інформує, засобами внутрішніх комунікацій банку, Службу сертифікації ЦСК щодо необхідності зміни статусу зареєстрованого підписувача на "анульований";
- служба сертифікації ЦСК скасовує сертифікат підписувача, формує СВС та поширює його в порядку, визначеному цим Регламентом.

## 12. Формування унікального розпізнавального імені підписувача

12.1. Служба сертифікації ЦСК формує унікальне розпізнавальне ім'я підписувача під час унесення даних про нього до реєстру ЦСК згідно з внутрішніми документів Банку, що відповідають вимогам законодавства України в сфері електронного цифрового підпису.

## 13. Генерування криптографічних ключів підписувача та запиту про формування сертифіката ключа

13.1. Відкритий та особистий ключі підписувача можуть бути згенеровані:

- на робочому місці підписувача;
- у ЦСК на робочій станції генерування ключів підписувачів (тільки для підписувачів, що є клієнтами Банку).

13.2. ЦСК у разі необхідності надає заявнику засоби ЕЦП для генерування криптографічних ключів та запитів про формування сертифіката ключа підписувача на його робочому місці. Запит про формування сертифіката ключа підписувача може бути лише у форматі PKCS#10 з накладеним ЕЦП з використанням особистого ключа підписувача.

13.3. Заявник генерує ключі підписувача на робочій станції генерування ключів, яка входить до складу ПТК ЦСК, якщо підписувач надав йому відповідні повноваження.

13.4. Підписувач, який є працівником банку, генерує свої криптографічні ключі на своєму робочому місці.

13.5. Згенерований особистий ключ підписувача захищається паролем та записується на НКІ. Підписувач несе відповідальність за забезпечення конфіденційності та цілісності особистого ключа. Заявник, якщо він виконував генерацію ключів, несе відповідальність за забезпечення конфіденційності та цілісності особистого ключа до моменту його передавання підписувачу.

## 14. Формування сертифіката ключа підписувача

14.1. ЦСК формує сертифікати ключів підписувачів тільки під час проведення процедури реєстрації підписувача або для зареєстрованих підписувачів у разі звернення підписувача/заявника з метою формування сертифіката ключа підписувача.

14.2. ЦСК формує сертифікати ключів підписувачів для відкритих ключів, що згенеровані відповідно до криптографічного алгоритму RSA.

14.3. Час розгляду документів, наданих для формування сертифіката ключа підписувача, зареєстрованого в ЦСК, становить не більше двох годин після її прийняття.

14.4. ЦСК здійснює формування сертифікатів ключів підписувачів у такому порядку:

14.4.1. Служба реєстрації ЦСК опрацьовує поданий заявником (підписувачем, який є працівником банку) запит про формування сертифіката ключа підписувача та документи згідно з вимогами цього Регламенту.

14.4.2. ЦСК приймає рішення про формування/відмову в формуванні сертифіката ключа підписувача.

14.4.3. Служба реєстрації ЦСК, в разі позитивного рішення ЦСК, вносить поданий заявником запит про формування сертифіката ключа підписувача до БД.

14.4.4. Служба сертифікації ЦСК формує сертифікати ключа підписувача в разі позитивного рішення ЦСК.

14.4.5. Процедура встановлення належності підписувачу особистого ключа та його відповідність відкритому ключу здійснюється шляхом перевірки ЕЦП у запиті про формування сертифіката ключа підписувача. Сертифікат ключа підписувача формується лише в разі підтвердження ЕЦП.

14.4.6. Служба сертифікації ЦСК під час формування сертифіката ключа підписувача:

- визначає дату і час початку та закінчення строку чинності сертифіката ключа підписувача;
- уносить до сертифіката ключа підписувача обов'язкові дані, визначені законодавством України в сфері електронного цифрового підпису та внутрішніми документами Банку;
- уносить до сертифіката ключа підписувача додаткові дані за зверненням заявника;

- уносить до сертифіката ключа підписувача інформацію щодо місця розміщення СВС на інформаційному ресурсі ЦСК;
- забезпечує унікальність реєстраційного номера сертифіката ключа в межах ЦСК, а також унікальність відкритих ключів у реєстрі чинних, блокованих та скасованих сертифікатів ключів.

14.4.7. Служба сертифікації ЦСК встановлює належність підписувачу особистого ключа та його відповідність відкритому ключу шляхом перевірки ЕЦП у запиті про формування сертифіката ключа підписувача. Сертифікат ключа підписувача формується лише в разі підтвердження ЕЦП.

14.4.8. Служба реєстрації ЦСК після формування сертифіката ключа підписувача надає його заявнику (підписувачу, який є працівником банку). Заявник (підписувач, який є працівником банку) повинен перевірити правильність відомостей, що містяться в сертифікаті ключа підписувача. У разі виявлення некоректних даних (помилки в реквізитах) він повинен повідомити про зазначене службу реєстрації ЦСК. У цьому разі сертифікат ключа скасовується та формується новий сертифікат ключа підписувача. У разі відсутності помилок підписувач візує Свідоцтво про достовірність сертифіката ключа (Додаток 1).

14.5. Служба сертифікації ЦСК здійснює поширення сертифіката ключа підписувача в установленому цим Регламентом порядку.

14.6. Заявник (підписувач, який є працівником банку) звертається до ЦСК щодо формування нового сертифіката ключа підписувача не пізніше ніж за десять робочих днів до закінчення строку чинності поточного сертифіката ключа підписувача. У разі неотримання заяви про формування нового сертифіката ключа підписувача у визначений термін ЦСК після закінчення строку чинності цього сертифіката скасовує його.

## 15. Формування сертифікатів ключів відповідальних осіб ЦСК

15.1. Відкритий та особистий ключі відповідальної особи ЦСК генеруються на її робочому місці. Під час генерування ключів автоматично створюється запит про формування сертифіката ключа.

15.2. Служба сертифікації ЦСК вносить запит відповідальної особи ЦСК про формування сертифіката ключа до БД ПТК ЦСК.

15.3. Служба сертифікації ЦСК під час формування нового сертифіката ключа формує та поширює СВС і після цього формує новий сертифікат ключа відповідальної особи ЦСК.

15.4. Відповідальна особа ЦСК не пізніше ніж за десять робочих днів до закінчення строку чинності поточного сертифіката ключа генерує нові криптографічні ключі та ініціює процедуру формування нового сертифіката ключа.

## 16. Формування сертифікатів ключів послуги інтерактивного визначення статусу сертифіката ключа

16.1. Служба сертифікації ЦСК здійснює генерування відкритих та особистих ключів послуги інтерактивного визначення статусу сертифіката ключа.

16.2. Служба сертифікації ЦСК вносить запити про формування сертифікатів ключів послуги інтерактивного визначення статусу сертифіката ключа до БД ПТК ЦСК.

16.3. Служба сертифікації ЦСК засвідчує запити про формування сертифікатів ключів послуги інтерактивного визначення статусу сертифіката ключа.

16.4. Служба сертифікації ЦСК не пізніше ніж за десять робочих днів до закінчення строку чинності поточного сертифіката ключа генерує нові криптографічні ключі та здійснює

процедуру формування нового сертифіката ключа послуги інтерактивного визначення статусу сертифіката ключа.

## 17. Формування сертифікату ключа послуги фіксування часу

17.1. Служба сертифікації ЦСК здійснює генерування відкритих та особистих ключів послуги фіксування часу і формує запит на створення сертифікату послуги фіксування часу.

17.2. ЦСК подає до служби реєстрації ЗЦ НБУ заяву на формування сертифіката ключа послуги фіксування часу та запит на створення сертифікату послуги фіксування часу.

17.3. Служба сертифікації ЗЦ НБУ засвідчує запит на формування сертифіката ключа послуги фіксування часу ЦСК.

17.4. Служба сертифікації ЦСК не пізніше ніж за десять робочих днів до закінчення строку чинності поточного сертифіката ключа генерує нові криптографічні відкриті та особисті ключі та ініціює процедуру формування в ЗЦ НБУ сертифіката ключа послуги фіксування часу ЦСК.

## 18. Зміна статусу сертифікатів ключів підписувачів

18.1. Зміна статусу сертифіката ключа підписувача набирає чинності з часу внесення відповідних змін до СВС та до реєстру чинних сертифікатів ключів підписувачів.

18.2. Підписувач зобов'язаний протягом не більше 30 календарних днів після блокування сертифіката ключа скасувати або поновити його. Поновлення сертифіката ключа підписувача можливе лише для сертифікатів, що заблоковані й термін блокування яких не закінчився. Якщо до закінчення терміну блокування сертифікат ключа не був поновлений, то ЦСК скасовує цей сертифікат ключа підписувача.

18.3. Дозволяється на розсуд підписувача скасувати сертифікат ключа без його блокування.

18.4. ЦСК блокує/поновлює сертифікат ключа підписувача в разі:

- подання заявником (підписувачем, який є працівником банку) звернення щодо блокування/поновлення сертифіката ключа підписувача до служби реєстрації ЦСК;
- наявності рішення суду про блокування/поновлення сертифіката ключа підписувача, що набрало законної сили.

18.5. ЦСК скасовує сертифікат ключа підписувача в разі:

- подання заявником (підписувачем, який є працівником банку) звернення про скасування сертифіката ключа підписувача до служби реєстрації ЦСК;
- наявності рішення суду про скасування сертифіката ключа підписувача, що набрало законної сили;
- смерті підписувача або оголошення його померлим за рішенням суду;
- визнання підписувача недієздатним за рішенням суду;
- припинення діяльності суб'єкта господарювання (якщо підписувач - клієнт банку, юридична особа чи фізична особа-підприємець);
- розірвання підписувачем трудового договору з юридичною особою, що є клієнтом банку (якщо сертифікат ключа виданий фізичній особі як представнику юридичної особи);
- надання заявником (підписувачем, який є працівником банку) недостовірних даних;

- не поновлення підписувачем заблокованого сертифіката протягом 30 календарних днів;
- припинення (розірвання) договору, на підставі якого підписувачу, який є клієнтом банку, надаються послуги ЕЦП.

18.6. Причинами, унаслідок яких підписувач звертається до служби реєстрації ЦСК щодо блокування/скасування сертифіката ключа підписувача, є:

- втрата або компрометація особистого ключа підписувача;
- втрата контролю за особистим ключем підписувача через компрометацію пароля доступу;
- зміна відомостей, зазначених у сертифікаті ключа;
- інші причини, визначені цим Регламентом та законодавством України у сфері ЕЦП.

18.7. Причинами, унаслідок яких підписувач звертається до служби реєстрації ЦСК щодо поновлення сертифіката ключа підписувача, є виявлення недостовірності даних про:

- втрату або компрометацію особистого ключа підписувача;
- втрату контролю за особистим ключем підписувача через компрометацію пароля доступу;
- зміну відомостей, зазначених у сертифікаті ключа.

18.8. Підписувач може подати до служби реєстрації ЦСК звернення щодо блокування сертифіката ключа підписувача у вигляді:

- письмової заяви;
- заяви в усній формі телефоном;

18.9. Підписувач подає до служби реєстрації ЦСК звернення щодо скасування сертифіката ключа підписувача у вигляді письмової заяви.

18.10. Підписувач подає заяву в усній формі засобами телефонного зв'язку за номерами ЦСК. У заяві в усній формі повідомляються:

- ідентифікаційні дані підписувача - власника сертифіката ключа підписувача;
- ідентифікаційні дані заявника (якщо підписувач та заявник є різними суб'єктами);
- серійний номер сертифіката ключа підписувача, що блокується;
- причина блокування;
- термін, на який блокується сертифікат ключа підписувача.

Блокування сертифіката ключа підписувача за заявою в усній формі здійснюється тільки в разі позитивної автентифікації заявника (збіг ідентифікаційних даних підписувача, заявника, серійного номера сертифіката ключа підписувача, переданої в усній заяві, з інформацією з реєстру ЦСК).

18.11. Заява про блокування сертифіката ключа підписувача в усній формі має бути підтверджена письмовою заявою протягом двох робочих днів з часу прийняття службою реєстрації ЦСК відповідного звернення. У разі ненадходження відповідної письмової заяви, що підтверджує блокування сертифіката ключа підписувача, протягом зазначеного терміну ЦСК блокує сертифікат ключа цього підписувача строком на 30 календарних днів.

18.12. Документи, що були підставою для зміни статусу сертифіката ключа підписувача, фіксуються та зберігаються в ЦСК.

18.13. Служба реєстрації ЦСК приймає письмові заяви про зміну статусу сертифіката ключа підписувача тільки протягом робочого дня ЦСК. Заяви про блокування сертифіката підписувача в усній формі приймаються цілодобово.

18.14. ЦСК здійснює зміну статусу сертифіката ключа підписувача в такому порядку:

18.14.1. Служба реєстрації ЦСК під час подання заявником заяви про зміну статусу сертифіката ключа підписувача:

- опрацьовує її згідно з вимогами цього Регламенту;
- створює запит про зміну статусу поточного сертифіката ключа підписувача в разі виконання заявником (підписувачем, який є працівником банку) усіх умов, визначених цим Регламентом.

18.14.2. Служба сертифікації ЦСК:

- уносить відповідні зміни до реєстру чинних сертифікатів ключів підписувачів із зазначенням дати, часу та причин зміни статусу сертифіката ключа підписувача;
- формує СВС;
- поширює інформацію про зміну статусу сертифіката ключа підписувача згідно з вимогами цього Регламенту.

18.14.3. ЦСК здійснює зміну статусу сертифіката підписувача протягом не більше двох годин з часу подання заяви в робочий час ЦСК. Заяви щодо зміни статусу сертифіката підписувача прийняті у неробочий час ЦСК обробляються наступного робочого дня ЦСК.

18.14.4. Заявник протягом трьох робочих днів (підписувач, який є працівником банку - протягом одного робочого дня) повідомляє ЦСК про зміну ідентифікаційних даних підписувача, які внесені до реєстру, шляхом подання відповідної заяви. Заявник (підписувач, який є працівником банку) разом із заявою про зміну ідентифікаційних даних підписувача подає заяву про формування нового сертифіката ключа підписувача в ЦСК, якщо дані, які змінюються, унесені до сертифіката ключа підписувача. Разом із заявою необхідно подати документи, що підтверджують ці зміни. ЦСК скасовує сертифікат ключа підписувача в разі неотримання від нього зазначеної заяви у визначений термін.

## 19. Зміна статусу сертифікатів ключів відповідальних осіб ЦСК

19.1. Зміна статусу сертифіката ключа відповідальної особи ЦСК набирає чинності з часу внесення відповідних змін до реєстру чинних сертифікатів ключів.

19.2. Строк блокування сертифікатів ключів відповідальних осіб ЦСК встановлює служба безпеки ЦСК. Цей строк не може перевищувати 30 робочих днів. Служба безпеки ЦСК може ініціювати скасування або поновлення заблокованого сертифіката ключа самостійно або за зверненням відповідальної особи ЦСК. Поновлення сертифіката ключа відповідальної особи ЦСК можливе лише для сертифікатів, що заблоковані й строк блокування яких не закінчився. Якщо до закінчення строку блокування сертифікат ключа не був поновлений, то ЦСК скасовує цей сертифікат ключа.

19.3. Дозволяється на розсуд служби захисту інформації ЦСК скасувати сертифікат ключа відповідальної особи ЦСК без його блокування.

19.4. Відповідальна особа ЦСК для зміни статусу свого сертифіката ключа звертається до служби захисту інформації ЦСК.

19.5. ЦСК змінює статус сертифіката ключа відповідальної особи ЦСК у разі позитивного рішення служби захисту інформації ЦСК.

19.6. Причинами, унаслідок яких відповідальна особа ЦСК звертається до служби захисту інформації ЦСК щодо блокування/скасування свого сертифіката ключа, є:

- компрометація особистого ключа, записаного на НКІ відповідальної особи ЦСК;
- вихід з ладу (фізичне пошкодження, збоїв під час роботи тощо) НКІ відповідальної особи ЦСК (якщо немає резервної копії цього НКІ);
- втрати НКІ відповідальною особою ЦСК;
- втрати або компрометація пароля доступу до НКІ відповідальної особи ЦСК;
- зміна відомостей, зазначених у сертифікаті ключа;
- інші причини, визначені цим Регламентом та законодавством України у сфері ЕЦП.

19.7. Причинами, унаслідок яких служба захисту інформації ЦСК звертається до служби сертифікації ЦСК щодо блокування/скасування сертифіката ключа відповідальної особи ЦСК, є:

- подання відповідальною особою ЦСК до служби захисту інформації ЦСК відповідної заяви;
- тривала відсутність відповідальної особи ЦСК на робочому місці (відпустка, хвороба тощо).

19.8. Причинами, унаслідок яких відповідальна особа ЦСК звертається до служби захисту інформації ЦСК щодо поновлення свого сертифіката ключа, є виявлення недостовірності даних про:

- втрату або компрометацію особистого ключа відповідальної особи ЦСК;
- втрату контролю за особистим ключем відповідальної особи ЦСК через компрометацію пароля доступу;
- зміну відомостей, зазначених у сертифікаті ключа.

19.9. Причинами, унаслідок яких служба захисту інформації ЦСК звертається до служби сертифікації ЦСК щодо поновлення сертифіката ключа відповідальної особи ЦСК, є подання відповідальною особою ЦСК до служби захисту інформації ЦСК заяви про поновлення сертифіката ключа.

19.10. Документи, що були підставою для зміни статусу сертифіката ключа відповідальної особи ЦСК, зберігаються в ЦСК.

19.11. Служба сертифікації ЦСК під час подання службою захисту інформації ЦСК рішення про зміну статусу сертифіката ключа відповідальної особи ЦСК:

- опрацьовує її згідно з вимогами цього Регламенту;
- уносить відповідні зміни до реєстру чинних сертифікатів ключів із зазначенням дати, часу та причин зміни статусу сертифіката ключа відповідальної особи ЦСК.

19.12. Служба сертифікації ЦСК здійснює зміну статусу сертифіката відповідальної особи ЦСК протягом не більше однієї години з часу подання рішення службою захисту інформації ЦСК.

19.13. Відповідальна особа ЦСК протягом одного робочого дня повідомляє службу захисту інформації ЦСК про зміну своїх ідентифікаційних даних, які внесено до реєстру.

Відповідальна особа ЦСК разом із заявою про зміну своїх ідентифікаційних даних подає заяву про формування нового сертифіката ключа, якщо дані, які змінюються, унесено до сертифіката ключа відповідальної особи ЦСК. Разом із заявою необхідно подати документи, що підтверджують ці зміни. ЦСК скасовує сертифікат ключа відповідальної особи ЦСК у разі неотримання зазначеної заяви у визначений термін.

## 20. Зміна статусу сертифікатів ключів послуги інтерактивного визначення статусу сертифіката

20.1. Зміна статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката набирає чинності з часу внесення відповідних змін у СВС та до реєстру чинних сертифікатів ключів.

20.2. Термін блокування сертифіката ключа послуги інтерактивного визначення статусу сертифіката установлює служба сертифікації ЦСК. Цей термін не може перевищувати 30 робочих днів. Поновлення сертифіката ключа послуги інтерактивного визначення статусу сертифіката можливе лише для сертифіката, що заблокований, і термін блокування якого не закінчився. Якщо до закінчення терміну блокування сертифікат ключа не був поновлений, то ЦСК скасовує цей сертифікат ключа.

20.3. Дозволяється на розсуд служби сертифікації ЦСК скасувати сертифікат ключа послуги інтерактивного визначення статусу сертифіката без його блокування.

20.4. Служба сертифікації ЦСК негайно блокує/скасовує сертифікат ключа послуги інтерактивного визначення статусу сертифіката у разі:

- втрати або компрометації особистого ключа послуги інтерактивного визначення статусу сертифіката;
- втрати контролю за особистим ключем послуги інтерактивного визначення статусу сертифіката через компрометацію пароля доступу;
- зміни відомостей, зазначених у сертифікаті ключа послуги інтерактивного визначення статусу сертифіката (зокрема, у зв'язку зі зміною даних ЦСК чи зміною налаштувань під час надання відповідних послуг).

20.5. Служба сертифікації ЦСК негайно поновлює сертифікат ключа послуги інтерактивного визначення статусу сертифіката у разі виявлення недостовірності даних про:

- втрату або компрометацію особистого ключа послуги інтерактивного визначення статусу сертифіката;
- втрату контролю за особистим ключем послуги інтерактивного визначення статусу сертифіката через компрометацію пароля доступу;
- зміни відомостей, зазначених у сертифікаті ключа послуги інтерактивного визначення статусу сертифіката.

20.6. Служба сертифікації ЦСК під час зміни статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката:

- створює запит на зміну статусу поточного сертифіката ключа послуги інтерактивного визначення статусу сертифіката та засвідчує його;
- уносить відповідні зміни до реєстру чинних сертифікатів ключів із зазначенням дати, часу та причин зміни статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката;
- формує СВС;

- поширює інформацію про зміну статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката згідно з вимогами цього Регламенту.

20.7. Служба сертифікації ЦСК виконує зміну статусу сертифіката послуги інтерактивного визначення статусу сертифіката протягом однієї години після прийняття цього рішення відповідно до причин, зазначених у цій главі.

20.8. Документи, що були підставою для зміни статусу сертифіката ключа послуги інтерактивного визначення статусу сертифіката, зберігаються в ЦСК.

## 21. Зміна статусу сертифікату ключа послуги фіксування часу

21.1. Зміна статусу сертифіката ключа послуги фіксування часу набирає чинності з часу внесення відповідних змін у СВС ЗЦ НБУ та до реєстру чинних сертифікатів ключів ЗЦ НБУ.

21.2. ЦСК для зміни статусу сертифіката ключа послуги фіксування часу подає заяву про зміну статусу відповідно до вимог Регламенту роботи ЗЦ НБУ, затвердженого постановою Правління Національного банку України 08 вересня 2014 року № 553 (зі змінами).

## 22. Блокування/розблокування відповідальних осіб ЦСК

22.1. Адміністратор служби захисту інформації ЦСК може заблокувати обліковий запис відповідальної особи ЦСК. У разі блокування облікового запису відповідальної особи ЦСК вона не має змоги працювати в ПТК ЦСК.

22.2. Блокування відбувається у випадках:

- звернення відповідальної особи ЦСК про блокування свого облікового запису;
- звільнення відповідальної особи ЦСК, зміна її функціональних обов‘язків або довготривалої відпустки – інформація надається Управління по роботі з персоналом.

22.3. Відповідальна особа ЦСК звертається до служби захисту інформації ЦСК про блокування свого облікового запису у разі:

- компрометації особистого ключа, записаного на НКІ відповідальної особи ЦСК;
- виходу з ладу (фізичного пошкодження, збоїв під час роботи тощо) НКІ відповідальної особи ЦСК (якщо немає резервної копії цього НКІ);
- втрати НКІ відповідальною особою ЦСК;
- втрати або компрометації пароля доступу до НКІ відповідальної особи ЦСК.

22.4. Відповідальна особа ЦСК звертається до служби захисту інформації ЦСК про розблокування свого облікового запису у разі виявлення недостовірності даних про:

- компрометацію особистого ключа, записаного на НКІ відповідальної особи ЦСК;
- вихід з ладу НКІ відповідальної особи ЦСК;
- втрату НКІ відповідальною особою ЦСК;
- втрату або компрометацію пароля доступу до НКІ відповідальної особи ЦСК.

## 23. Інформаційний ресурс ЦСК

23.1. Інформаційний ресурс ЦСК призначено для розміщення на ньому відкритої інформації, яка структурно поділяється на:

- довідкову інформацію (режим роботи ЦСК, положення Регламенту роботи ЦСК, нормативні документи тощо);
- сертифікати ключів ЦСК;
- СВС, що містить інформацію про статус сертифікатів ключів ЦСК та підписувачів;

23.2. Публікація СВС і сертифікатів ключів ЦСК на інформаційному ресурсі ЦСК та HTTP-сервері здійснюється впродовж п’яти хвилин після їх формування та перевірки власником сертифіката/заявником даних, що вносяться до сертифіката ключа.

23.3. Довідкова інформація розміщується на інформаційному ресурсі ЦСК на HTTP-сервері у вигляді набору веб-сторінок.

23.4. Сертифікати ключів ЦСК, а також СВС розміщуються у складі веб-сторінок на HTTP-сервері інформаційного ресурсу ЦСК;

23.5. Доступ до HTTP-сервера здійснюється за DNS-ім'ям ocspext.eximb.com за протоколом HTTP (номер TCP-порту 9080).

## 24. Зовнішні інтерфейси, протоколи і формати обміну даними

24.1. У ПТК ЦСК застосовано такі операційні протоколи обміну для підтримки експорту-імпорту даних у ЦСК:

- HTTP використовують для надання доступу до інформаційного ресурсу ЦСК;
- SMTP, POP3 використовують для обміну електронними поштовими повідомленнями між ЦСК і підписувачами.

## 25. Поширення інформації про статус сертифікатів ключів

25.1. ЦСК поширює інформацію про статус сертифіката ключа:

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

25.2. 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 електронного цифрового підпису. Підписувач на свій розсуд може використовувати клієнтське ПЗ, яке вільно поширюється шляхом його розміщення на інформаційному ресурсі ЦСК, розроблене самостійно чи створене сторонніми розробниками.

25.3. ЦСК під час формування СВС забезпечує таке:

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

25.4. ЦСК поширює СВС шляхом їх розміщення на інформаційному ресурсі ЦСК 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.

25.5. Перед використанням сертифіката ключа підписувача слід перевірити:

- чинність цього сертифіката ключа на момент накладення електронного цифрового підпису на документ;
- електронний цифровий підпис у сертифікаті ключа (за допомогою сертифіката власного ключа ЦСК, чинного на момент формування цього сертифіката ключа);
- статус сертифіката ключа підписувача за поточним СВС або за допомогою OCSP-запиту;
- автентичність і цілісність СВС та/чи отриманої OCSP-відповіді.

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

## 26. Послуги фіксування часу

26.1. У ЦСК послуги фіксування часу надаються з використанням TSP-сервера.

26.2. Взаємодія з TSP-сервером для отримання послуг фіксування часу забезпечується шляхом використання клієнтського ПЗ. Таке ПЗ повинно відповідати технічним специфікаціям та форматам даних, визначеним законодавством України у сфері електронного цифрового підпису. Підписувач на свій розсуд може використовувати клієнтське програмне забезпечення, яке поширюється шляхом його розміщення на інформаційному ресурсі ЦСК, розроблене самостійно чи створене сторонніми розробниками.

## 27. Синхронізація часу в ПТК ЦСК

27.1. 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).

27.2. ЦСК синхронізує час із серверами часу Національного банку України.

27.3. ПТК ЦСК забезпечує синхронізацію із всесвітнім координованим часом (UTC) з точністю до однієї секунди за допомогою мережевого протоколу NTP. Алгоритм корекції часу в ПТК ЦСК з використанням NTP включає внесення затримок, корекцію частоти годинника і ряд механізмів, що дають змогу досягти необхідної точності під час синхронізації часу в ПТК ЦСК, навіть після тривалих періодів втрати зв'язку із сервером часу. ПТК ЦСК працює за київським часом з автоматичною поправкою на літній та зимовий періоди.

27.4. Системний адміністратор ЦСК налаштовує NTP з використанням засобів операційної системи.

## 28. Порядок архівного зберігання документованої інформації

28.1. ЦСК здійснює архівне зберігання таких документів:

- сертифікати ключів ЦСК, відповідальних осіб ЦСК та підписувачів (чинні, скасовані, блоковані);
- реєстр відповідальних осіб ЦСК та підписувачів;
- копії і оригінали документів на папері та документи в електронному вигляді, що подані заявниками (підписувачами, які є працівниками банку) під час реєстрації, формування, зміни статусу сертифіката ключа, зміни даних підписувачів;
- СВС;
- запити на формування позначок часу і самі позначки часу;

- запити на визначення статусу сертифікатів ЦСК та підписувачів і квитанції-відповіді на ці запити;
- журнали аудиту та документи ЦСК, у тому числі протоколи роботи ПТК ЦСК.

28.2. ЦСК зберігає документи на паперових носіях у порядку, установленому законодавством України про архіви й архівну справу. ЦСК зберігає електронні копії БД та журналів аудиту на окремих знімних носіях у приміщенні, захищеному від несанкціонованого доступу.

28.3. Сертифікати ключів ЦСК, відповідальних осіб ЦСК, підписувачів та СВС є документами постійного зберігання.

28.4. Інші документи, що підлягають архівному зберіганню, є документами тимчасового зберігання. Термін зберігання архівних документів становить п'ять років.

28.5. Виділення архівних документів до знищення та саме знищення виконуються комісією за безпосередньою участю керівника ЦСК та адміністратора безпеки ЦСК або уповноважених ними відповідальних осіб ЦСК. За фактом проведення процедури знищення архівних документів складається відповідний акт.

28.6. ЦСК надає доступ до необхідного сертифіката та пов'язаних з ним СВС з архівних записів ЦСК за запитом заявників у строки, установлені законодавством України для відповідей на звернення громадян.

## 29. Порядок унесення змін до Регламенту

29.1. Зміни до цього Регламенту вносяться відповідно до законодавства України.

29.2. У разі внесення змін до цього Регламенту відповідальні особи ЦСК та підписувачі інформуються про це шляхом розміщення оновленого Регламенту та об'яви про відповідні зміни на інформаційному ресурсі ЦСК;

29.3. Зміни до цього Регламенту можуть бути проведені внаслідок зміни законодавства України з питань ЕЦП, розвитку відповідних інформаційних технологій, появи нових міжнародних і національних стандартів України, виправлення помилок тощо.

Додаток 1.

# Свідоцтво про достовірність сертифіката ключа

**Власник сертифіката:**

```
E = mpup@gmail.com
CN = pupkin1234
SURNAME = Пупкін Мар’ян Адольфович
C = UA
```

**Дійсний з** `YYYY-MM-DD HH:mm:SS+03:00` **по** `YYYY-MM-DD HH:mm:SS+03:00`

**Серійний номер:** `XX XX XX XX XX XX XX XX`

**Відкритий ключ користувача:**

```
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
        XX XX XX XX XX XX XX XX
```

Будь-який електронний документ, що містить електронний цифровий підпис, перевірка якого з використанням цього сертифіката відкритого ключа дає позитивний результат, вважається підписаним особисто мною:

(підпис власника сертифіката)

*Підпис власника та достовірність сертифіката завіряю:*
*(заповнюється лише клієнтом-юридичною особою)*

(прізвище та ініціали керівника) (підпис/печатка) "____"_____20____р.

*Підписи відповідають зразкам:*
*(заповнюється банком)*

(прізвище та ініціали менеджера) (підпис) "____"_____20____р.