ЗАТВЕРДЖЕНО

В.о. Голови Правління
ПАТ «КРЕДОБАНК»

_____ І. Шатковскі

«16» січня 2016 року

ПОГОДЖЕНО

Заступник Голови Правління
Національного Банку України,
керівник Засвідчувального центру
Національного банку України

_____ Я. В. Смолій

«3» березня 2016 року

Регламент роботи центру сертифікації ключів ПАТ «КРЕДОБАНК»

ПОГОДЖЕНО

Директор Департаменту
інформаційних
технологій ПАТ «КРЕДОБАНК»

_____ А.О. Андрушко

«15» січня 2016 року

ПОГОДЖЕНО

Директор Департаменту банківської
безпеки ПАТ «КРЕДОБАНК»

_____ О.С. Горінов

«16» січня 2016 року

Львів 2016

В цьому Регламенті роботи ЦСК ПАТ "Кредобанк" зав'язано п'ятдесят один аркуш.

Старший інженер Департаменту безпеки
Національного банку України Кабиш Ю.М.

ЗМІСТ

Цей Регламент ЦСК (далі-Регламент) визначає порядок та процедури обслуговування сертифікатів відкритих ключів (далі – сертифікатів) підписувачів (клієнтів та співробітників банку), умови надання послуг та правил користування послугами ЦСК, а також основні організаційно-технічні заходи, що направлені на забезпечення функціонування ЦСК.

Регламент розроблено відповідно до чинного законодавства України у сфері електронного цифрового підпису, а саме:

- Закону України «Про електронний цифровий підпис»;
- Порядку засвідчення наявності електронного документу (електронних даних) на певний момент часу, затвердженого постановою Кабінету Міністрів України від 26 травня 2004 року № 680;
- Правил оформлення Регламенту роботи центрів сертифікації ключів банків України, затверджених постановою Правління Національного банку України від 17.06.2010 № 284;
- Примірного регламенту роботи центрів сертифікації ключів банків України, затвердженого постановою Правління Національного банку України від 17.06.2010 № 284 (зі змінами);
- Положення про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України, затвердженого постановою Правління Національного банку України від 17.06.2010 № 265 (зі змінами)
- Правила передавання центрами сертифікації ключів документованої інформації до Засвідчувального центру Національного банку України, затверджені постановою Правління Національного банку України від 07.07.2015 № 440.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Визначення скорочень

АБС – автоматизована банківська система;

БД - база даних;

ВПР – віддалений пункт реєстрації;

ДБО – дистанційне банківське обслуговування;

ДББ – Департамент банківської безпеки;

ДІТ – Департамент інформаційних технологій;

ДЕЛ – Департамент електронного бізнесу;

ЕЦП – електронний цифровий підпис;

Заявник – заявник підписувача, що є клієнтом банку;

ІТС – інформаційно-телекомунікаційна система;

НГМД – накопичувач на гнучких магнітних дисках;

НЖМД – накопичувач на жорстких магнітних дисках;

НЖМОД – накопичувач на жорстких магніт-оптичних дисках;

НКІ – носій ключової інформації;

ПЗ – програмне забезпечення;

ПТК – програмно-технічний комплекс;

РС – робоча станція;

СВС – список відкликаних сертифікатів;

СЗІ – система захисту інформації;

СУБД – система управління БД;

ЦР – центр реєстрації;

ЦОД – центр обробки даних;

ЦПД – центр приймання дзвінків;

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 інтерактивного визначення статусу сертифіката;

POP3 – поштовий протокол версії 3;

SMTP – простий протокол передавання електронної пошти;

TCP – протокол керування передаванням;

TSP – протокол фіксування часу.

1.2. Визначення термінів

ВЛАСНИКИ ТЕХНОЛОГІЧНИХ КЛЮЧІВ І СЕРТИФІКАТІВ, А ТАКОЖ ПОСАДОВЦІ КЛІЄНТА (ДИРЕКТОР, БУХГАЛТЕР) - власники особистих ключів і сертифікатів, при спільній згадці позначаються як користувачі;

ДОГОВІР, ВІДПОВІДНО ДО ЯКОГО ПІДПИСУВАЧУ НАДАЮТЬСЯ ПОСЛУГИ ЕЦП – окремий договір про надання послуг ЕЦП або договір про обслуговування клієнта банку, що має містити договір про надання послуг ЕЦП підписувачу. Підписувачі, які є працівниками банку, не укладають з ЦСК договір про надання послуг ЕЦП;

ЗАЯВНИК – уповноважений представник підписувача, який є клієнтом банку, у ЦСК, який на законних підставах звертається до ЦСК з метою організації та проведення реєстрації підписувача - клієнта банку формування та зміни статусу його сертифіката, а також зміни його даних (реквізитів) в установленому порядку. Якщо в основних даних (реквізитах) сертифіката 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 ЦСК;

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

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

СЗІ ПТК ЦСК - сукупність організаційних заходів, інженерно-технічних 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 власного ЦСК. Банк призначає підписувача - працівника банку розпорядчим документом;

ПОНОВЛЕННЯ СЕРТИФІКАТА - процедура управління статусом сертифіката, що поновлює чинність сертифіката (якій передувала відповідна процедура блокування сертифіката);

ПТК ЦСК - сукупність технічного обладнання, ПЗ, що використовується 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 в ЦСК цих документів і формування сертифікату підписувача – клієнта банку;

ПРОЦЕДУРА РЕЄСТРАЦІЇ ПІДПИСУВАЧА, ЯКИЙ Є ПРАЦІВНИКОМ БАНКУ - установлена процедура подання ним до ЦСК необхідного пакета документів, опрацювання в ЦСК цих документів і формування сертифікату підписувача - працівника банку;

СЕРТИФІКАТ ВІДПОВІДАЛЬНОЇ ОСОБИ ЦСК - сертифікат відповідальної особи ЦСК, чинність якого засвідчується особистими ключами ЦСК;

СКАСУВАННЯ СЕРТИФІКАТУ - процедура управління статусом сертифікату, яка зупиняє чинність сертифіката;

СТРОК ЧИННОСТІ СЕРТИФІКАТУ - проміжок часу між датою і часом початку та датою і часом закінчення чинності сертифіката, що встановлюються під час формування сертифікату;

СТРОК ЧИННОСТІ ОСОБИСТОГО КЛЮЧА - строк, протягом якого використання особистого ключа є чинним.

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.

1.3. Сфера дії документу

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

1.4. Доступ до документу (поширення або розповсюдження)

Положення цього Регламенту поширюються в електронній формі:

- шляхом розміщення на інформаційному ресурсі ЦСК (http://ca.kredobank.com.ua);
- засобами електронної пошти (e-mail), що надсилаються відповідальною особою ЦСК.

1.5. Суб'єкти відносин

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

1.6. Причетні сторони

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:

- Відповідальні особи ЦСК.
- Підписувачі, що є співробітниками банку.
- Підписувачі, що не є співробітниками банку – клієнти банку.

1.7. Ідентифікаційні дані ЦСК

Повне найменування організації	Публічне акціонерне товариство «КРЕДОБАНК»
Скорочене найменування організації	ПАТ «КРЕДОБАНК»
ЄДРПОУ	09807862
Місцезнаходження організації	Луганська 16, м. Львів Україна, 79026
Номер телефону	0-800-500-8-50, (032) 297-23-45
Повне найменування ЦСК	Центр сертифікації ключів ПАТ «КРЕДОБАНК»
Скорочене найменування ЦСК	ЦСК ПАТ «КРЕДОБАНК»
Юридична адреса організації	вул. Сахарова 78, м. Львів Україна, 79026
Веб-сайт ЦСК	http://ca.kredobank.com.ua
Електронна поштова скринька ЦСК	csk@kredobank.com.ua

2. ОРГАНІЗАЦІЙНА СТРУКТУРА ЦСК

2.1. Загальні положення

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

2.2. Адміністративні функції

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 їх діяльності, до ЗЦ НБУ.

2.3. Технічні та технологічні функції

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 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 та відкритих ключів послуги фіксування часу в ЗЦ НБУ;
- формування сертифікатів сервісу OCSP ЦСК, відповідальних осіб ЦСК і підписувачів;
- ведення реєстру ЦСК;
- поширення сертифікатів ЦСК і підписувачів у встановленому цим Регламентом порядку;

- блокування, скасування та поновлення сертифікатів сервісу OCSP ЦСК, формування відповідного запиту до ЗЦ НБУ на формування сертифікату TSP, відповідальних осіб ЦСК і підписувачів у випадках, передбачених цим Регламентом і законодавством України у сфері ЕЦП;
- надання послуг інтерактивного визначення статусу сертифіката;
- інші дії, пов'язані з технічною та технологічною підтримкою діяльності ЦСК.

2.4. Служби ЦСК

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

- служба захисту інформації;
- служба сертифікації ;
- служба реєстрації;
- служба системного адміністратора;
- центр приймання дзвінків відділу обслуговування клієнтів IFOBS ДЕЛ.

2.5. Основні функції служби захисту інформації

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

Функцій та завдання служби захисту інформації ЦСК приведені у Положенні про Службу захисту інформації.

ВПР розгортаються у відділеннях банку, де призначаються співробітники, які відповідають за захист інформації в ІТС ВПР.

2.6. Основні функції служби сертифікації

- вивантаження з ПТК ЦСК власних і відкритих ключів ЦСК для засвідчення їх чинності в ЗЦ НБУ;
- завантаження сертифікатів власних ключів ЦСК в ПТК ЦСК;
- звернення до ЗЦ НБУ щодо зміни статусу власних сертифікатів ЦСК та сертифікатів послуги фіксування часу у випадках, передбачених цим Регламентом і законодавством України у сфері ЕЦП;
- надання послуг визначення статусу сертифікатів ЦСК і підписувачів користувачам послуг ЕЦП;
- надання відповідальним особам ЦСК послуг визначення статусу сертифікатів відповідальних осіб ЦСК;
- генерування ключів ЦСК;
- перехід на використання нових ключів ЦСК;
- знищення особистих ключів ЦСК, строк чинності яких закінчився;
- засвідчення чинності відкритих ключів сервісу OCSP, відповідальних осіб ЦСК, підписувачів;
- управління статусом сертифікатів сервісів OCSP, TSP, відповідальних осіб ЦСК, підписувачів.

2.7. Основні функції служби реєстрації

- опрацювання документів, які подаються заявником до ЦСК під час проведення процедур реєстрації, формування сертифікатів, зміни статусу сертифікатів, 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, зміни статусу сертифікатів, зміни його ідентифікаційних даних;
- надання допомоги під час генерування ключів підписувачів у разі потреби та вживання заходів щодо забезпечення безпеки інформації під час генерування;
- уведення в ПТК ЦСК запитів на формування сертифікатів підписувачів для виконання засвідчення їх чинності;
- генерування в ПТК ЦСК запитів на блокування, скасування чи поновлення сертифікатів під час подання відповідних заяв;
- розгляд скарг підписувачів.

ВПР розгортаються у відділеннях банку, де призначаються співробітники, які виконують функції служби реєстрації (оператори реєстрації).

2.8. Основні функції служби системного адміністратора

- установлення та налаштування ОС, серверних і клієнтських застосувань на серверній техніці та робочих місцях відповідальних осіб ЦСК;
- виконання оновлень ПЗ ПТК ЦСК;
- вивантаження/завантаження резервної інформації із/в ПТК ЦСК;
- налаштування точного часу на серверах та робочих станціях ЦСК;
- ведення централізованих резервних копій налаштувань, даних для серверів ЦСК;
- підтримка належного функціонування ПТК ЦСК.

2.9. Автоматизовані робочі місця ЦСК

У ЦСК для виконання завдань, покладених на зазначені в пункті 2.4 цього Регламенту, створено такі автоматизовані робочі місця:

- автоматизоване робоче місце адміністратора безпеки ЦСК;
- автоматизоване робоче місце адміністратора сертифікації ЦСК;
- автоматизоване робоче місце адміністратора реєстрації ЦСК;
- автоматизоване робоче місце системного адміністратора ЦСК;
- автоматизоване робоче місце реєстратора у відділеннях банку;
- автоматизоване робоче місце оператора центру приймання дзвінків;
- неспеціалізовані автоматизовані робочі місця.

Відповідальні особи ЦСК виконують функції зазначених у пункті 2.4 цього Регламенту служб на відповідних автоматизованих робочих місцях.

Відповідальні особи ЦСК виконують роботу з нормативно - довідковою інформацією ЦСК на своїх спеціалізованих автоматизованих робочих місцях або на неспеціалізованих автоматизованих робочих місцях відповідно до вимог, визначених політикою безпеки інформації ЦСК і наданих їм адміністратором безпеки ЦСК повноважень.

Відповідальна особа ЦСК, що є адміністратором безпеки ЦСК, не може суміщати свої функції з функціями інших відповідальних осіб.

Служба безпеки ЦСК надає доступ до АРМ реєстратора у відділеннях банку для генерування стартових ключів підписувачу, який є клієнтом або працівником банку. Робота з АРМ реєстратора з відділень банку відбувається в межах термінальної сесії до опублікованого АРМ реєстратора у середовищі Citrix.

Підписувачі, які є клієнтами або працівниками банку, отримують стартові ключі у відділенні банку, а зміну стартових ключів і першу реєстрацію запитів на формування робочого сертифікату відбувається на робочому місці, згідно з політикою безпеки ЦСК.

Усі відповідальні особи ЦСК перед початком виконання своїх функціональних обов'язків

повинні ознайомитися зі змістом цього Регламенту, інструкціями щодо експлуатації АРМів, інструкціями щодо забезпечення безпеки експлуатації НКІ та порядком генерування ключових даних і роботи з ключами. Відповідальні особи ЦСК підтверджують факт ознайомлення з цими документами особистим підписом.

3. АРХІТЕКТУРА ПТК ЦСК

3.1. Логічна архітектура ПТК ЦСК

ЦСК банку будується на основі системи криптографічного захисту інформації (СКЗІ) «Шифр-Х.509», яка складається з трьох підсистем:

- підсистеми управління ключами;
- підсистеми криптографічного захисту даних;
- підсистеми організаційно-технічного захисту.

СКЗІ «Шифр-Х.509» забезпечує:

- управління ключами ЕЦП та відповідними сертифікатами, вироблення спільного ключа;
- формування і перевірку ЕЦП;
- управління ключами вироблення спільного секрету;
- шифрування і розшифрування даних, їх імітозахист;
- формування і перевірку позначок часу.

3.1.1. Підсистема управління ключами

Підсистема управління ключами, рис.1, складається з наступних засобів:

- ПЗ сертифікації ключів,
- ПЗ центру реєстрації,
- ПЗ LDAP-сервер;
- ПЗ сервер OCSP;
- ПЗ сервер TSP;
- ПЗ АРМ реєстратора;
- ПЗ АРМ оператора Центру приймання дзвінків;
- ПЗ АРМ адміністратора сертифікації;
- ПЗ АРМ звітності ЦСК;
- ПЗ АРМ адміністратора безпеки;
- ПЗ Комунікаційний модуль;
- ПЗ АРМ адміністратора реєстрації;
- ПЗ АРМ системного адміністратора;
- ПЗ Системи резервного копіювання;
- ПЗ Служби реплікації даних.
- ПЗ ВПР.

3.1.2. ПТК ЦСК

ПТК ЦСК призначений для реалізації регламентних процедур і механізмів роботи ЦСК, пов'язаних з обслуговування сертифікатів, які включають:

- управління ключами ЦСК.
- реєстрацію користувачів;
- сертифікацію відкритих ключів користувачів;
- розповсюдження сертифікатів;
- управління статусом сертифікатів;

- надання інформації про статус сертифікату;
- надання послуг позначок часу;
- виконання синхронізації даних БД;
- виконання моніторингу і діагностики компонентів ПТК ЦСК;
- виконання централізованого резервного копіювання даних.

ПТК ЦСК функціонує на базі основного ЦОД та резервного ЦОД.

Основний ЦОД знаходиться за адресою: Україна, м. Львів, вул.Сахарова 78а, тел. (032) 2977891.

Резервний ЦОД знаходиться за адресою: Україна, м. Львів, вул. Луганська 16, тел. (032) 2977891.

Переключення між основним та резервними ЦОД виконується за відповідним регламентом.

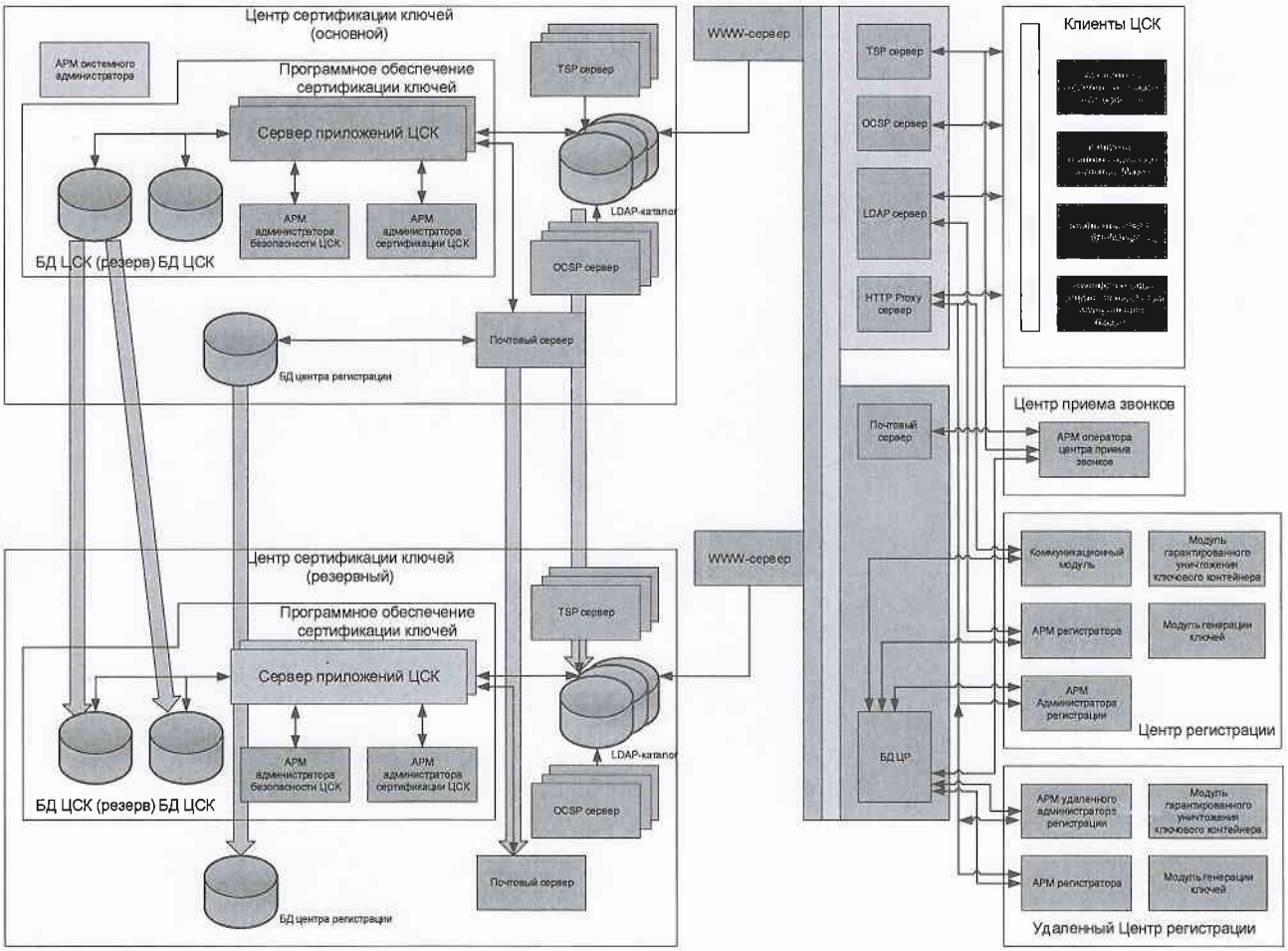

Рис. 1. Підсистема управління ключами

3.1.3. ПЗ сертифікації ключів

3.1.3.1.Склад ПЗ сертифікації ключів наступний:

- АРМ адміністратора безпеки;
- АРМ адміністратора сертифікації;
- АРМ звітності ЦСК;
- Сервер застосувань ЦСК;
- БД ЦСК;
- Спільний довідник сертифікатів на базі LDAP-каталогу.

3.1.3.2. Основними функціями ПЗ сертифікації ключів є:

- управління ключами посадових осіб ЦСК;
- управління ключами ЦСК;
- створення і контроль функціонування ЦР, видача стартових ключів операторам реєстрації, адміністраторам реєстрації, операторам ЦПД;
- приймання і автентифікація запитів на формування сертифікатів;
- перевірка на унікальність відкритих ключів прийнятих у запитах на формування сертифікатів;
- сертифікація відкритих ключів користувачів;
- управління статусом сертифікатів ;
- передача сертифікатів і СВС до ЦР;
- ведення БД сертифікатів, а також запитів на формування сертифікату, запитів на блокування, поновлення і скасування сертифікатів;
- управління довідником сертифікатів: розміщення, видалення сертифікатів у LDAP-каталозі;
- видача позначок часу.

3.1.4. Програмні засоби ЦР

ПЗ ЦР призначені для ідентифікації і реєстрації користувачів, які звертаються за сертифікатами, та для надання послуг генерації ключів користувачів, які забажали виконати цю процедуру безпосередньо у ЦР.

3.1.4.1.ПЗ ЦР складається з наступних програмних засобів:

- АРМ адміністратора реєстрації;
- АРМ реєстратора;
- БД ЦР;
- Комунікаційний модуль;
- Модуль генерації ключів користувачів.

3.1.4.2.Основними функціями ЦР є:

- розмежування доступу до функцій і даних ЦР;
- управління ключами адміністратора реєстрації;
- управління ключами операторами реєстрації;
- ідентифікація і реєстрація користувачів;
- видання стартових сертифікатів користувачам;
- генерація робочих ключів для користувачів, які захотіли отримати робочі сертифікати безпосередньо у ЦР, формування відповідних запитів на формування сертифікатів;
- приймання і перевірка автентичності запитів на формування сертифікатів користувачів;
- підтвердження запитів на формування сертифікатів користувачів підписом оператора реєстрації;
- підтвердження запитів на формування сертифікатів користувачів підписом адміністратора реєстрації;
- передача запитів на формування сертифікатів до ЦСК електронною поштою або експорт у вигляді файлів у вказаний каталог (на носій);
- формування запитів на скасування, блокування, поновлення дії сертифікатів;
- підтвердження запитів на скасування, блокування, поновлення дії сертифікатів підписом адміністратора реєстрації та їх передача до ЦСК або експорт у вигляді файлів у вказаний каталог (на носій);
- приймання і контроль автентичності сертифікатів користувачів і СВС;
- видача сертифікатів користувачів, які захотіли отримати їх безпосередньо у ЦР;
- передача сертифікатів і СВС на адресу користувачів, які генерують свої ключі самостійно;

- ведення і аудит локальної БД сертифікатів, а також запитів на формування сертифікату і запитів на блокування, поновлення і скасування сертифікатів;
- управління локальним довідником сертифікатів (якщо такий створюється): розміщення, видалення сертифікатів у LDAP-каталозі.

3.1.5. LDAP-сервер

LDAP-сервер (каталог) призначений для створення довідника сертифікатів ЦСК. LDAP-сервер забезпечує зберігання і надання доступу користувачам за протоколом TCP/IP до опублікованих сертифікатів і СВС, які видаються ЦСК.

3.1.6. Сервер OCSP

Сервера OCSP призначений для передачі користувачам інформації про статус сертифіката у інтерактивному режимі за протоколом TCP/IP. OCSP-сервер функціонує у відповідності до рекомендацій RFC2560 «Online Certificate Status Protocol – OCSP».

3.1.7. Сервер TSP

Сервера TSP призначено для формування і передачі користувачам міток часу електронних документів в інтерактивному режимі за протоколом TCP/IP. TSP-сервер функціонує у відповідності до рекомендацій RFC3161 «Time-Stamp Protocol - TSP».

3.1.8. АРМ оператора ЦПД

АРМ оператора ЦПД призначено для виконання дій, пов'язаних з управління статусом сертифікатів за вимогою користувачів, яким ці сертифікати належать.

Основними функціями АРМ оператора ЦПД є:

- пошук і відбір сертифікатів для зміни їх статусу у відповідності із заявами користувачів;
- формування запитів на відклик, блокування, поновлення дії сертифікатів;
- підтвердження запитів на скасування, блокування, поновлення дії сертифікатів підписом оператора ЦПД і їх передача до ЦСК.

3.1.9. Програмні засоби ВПР

Для наближення послуг з видання сертифікатів користувачам, які територіально віддалені від ЦСК, розгортаються ВПР.

ВПР за складом ПЗ, та за виконуваними функціями, ідентичні програмним засобам ЦР, які функціонують у складі ЦСК (див. розділ Програмні засоби ЦР).

3.2. Програмно-технічний комплекс ЦСК Банку

ПТК ЦСК банку є автоматизованою системою класу 3. На рис. 2 наведено схему розгортання серверів та робочих місць ЦСК.

Технічні засоби комплексу об'єднанні у розподілену обчислювальну мережу з використання інформаційної мережі банку, частина з яких підключена до зовнішніх телекомунікаційних мереж, рис. 3.

3.3. Апаратне комп'ютерне забезпечення ПТК ЦСК

Апаратне забезпечення ПТК ЦСК банку складається з двох типів обладнання:

- серверів;
- робочих станцій.

Сервери розгорнуті у віртуальній інфраструктурі банку у основному ЦОД та резервному ЦОД.

Клієнтські робочі станції представляють собою або окремі фізичні робочі станції, або

віртуальні, доступ до яких відбувається за допомогою віддаленого доступу.

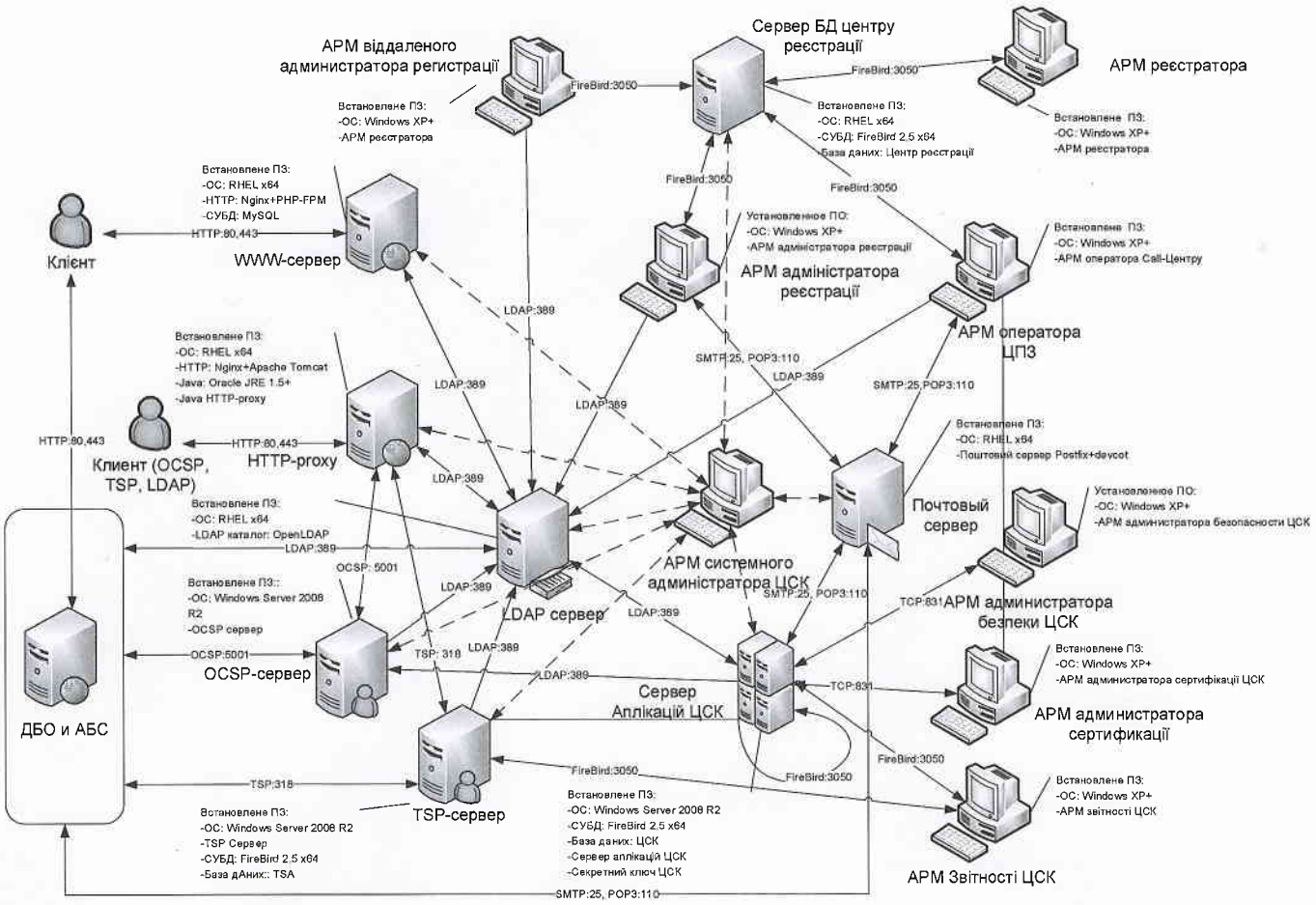

Рис. 2. Схема взаємодії серверів та робочих станцій ЦСК

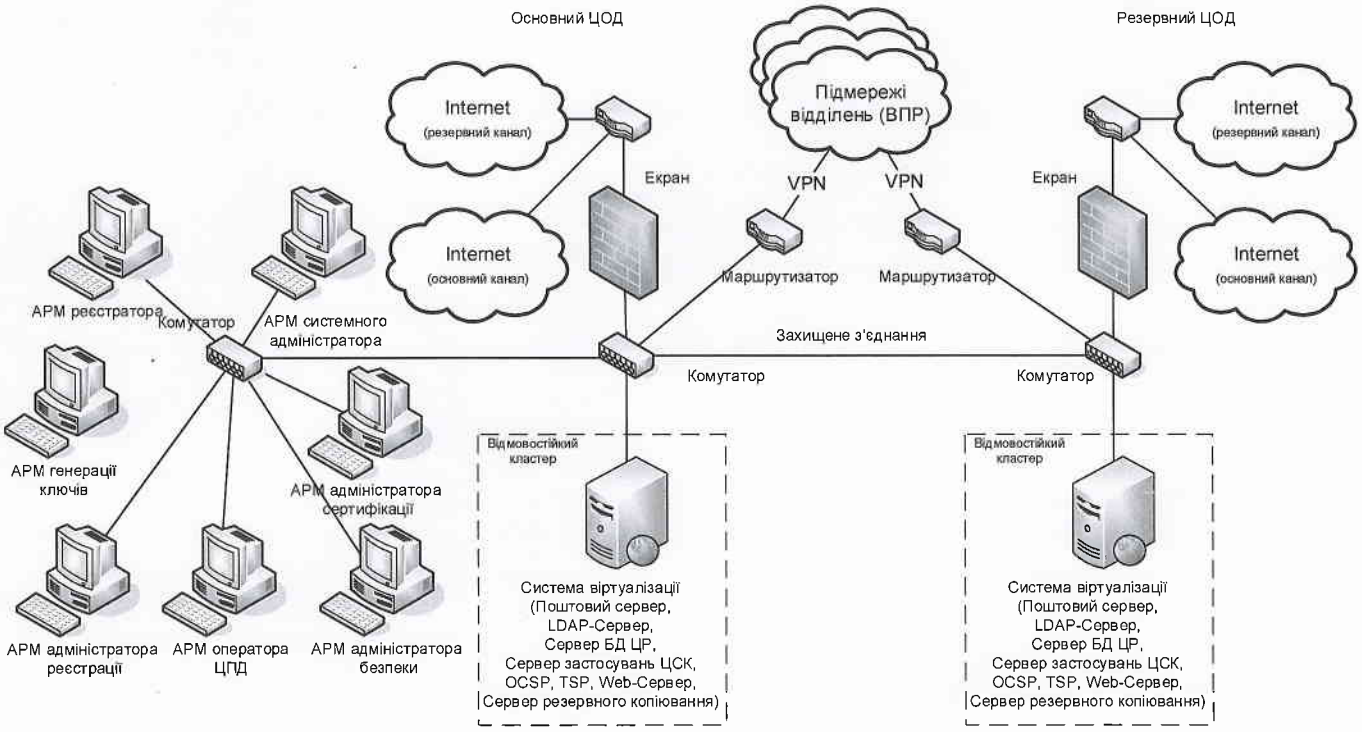

Рис. 3. Топологія мережі ПТК ЦСК банку

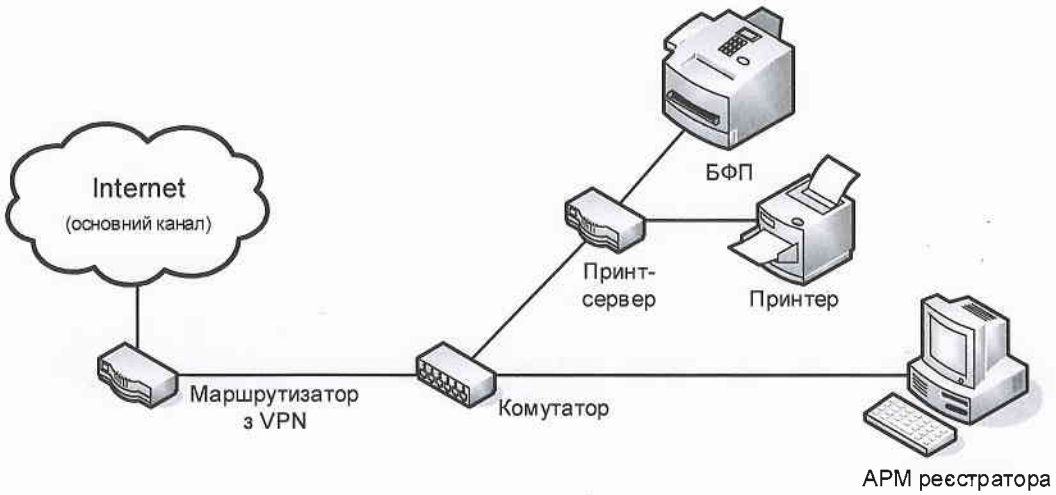

Рис. 4. Топологія мережі ПТК ВПР у відділенні банку

3.4. Програмне забезпечення ПТК ЦСК банку

Програмне забезпечення ПТК ЦСК банку є централізованим і відповідає багатоланковій (багаторівневій) архітектурі, що складається з наступних компонентів:

- Серверне ПЗ сертифікації:
  - Сервер застосувань ЦСК.
  - СУБД для БД ЦСК.
  - Сервер OCSP.
  - Сервер TSP.
  - LDAP-сервер.
- Серверне ПЗ реєстрації:
  - СУБД для БД ЦР.
  - Комунікаційний модуль.
- Серверне ПЗ інфраструктури:
  - Поштовий сервер.
  - Сервер реплікації даних.
  - Сервер резервного копіювання.
- Клієнтське ПЗ сертифікації:
  - АРМ адміністратора безпеки.
  - АРМ адміністратор сертифікації.
  - АРМ звітності ЦСК.
- Клієнтське ПЗ реєстрації:
  - АРМ реєстратора.
  - АРМ адміністратора реєстрації.
- Клієнтське ППЗ інфраструктури:
  - АРМ системного адміністратора.

3.5. Розгортання програмного забезпечення ПТК ЦСК Банку

Відповідно до схеми розгортання ПТК ЦСК, рис. 2, БД ЦР, БД ЦСК та клієнтські компоненти доступу до них, разом з іншими серверними застосуваннями розміщуються і

функціонують на серверному обладнанні.

Усі інші клієнтські застосування, що використовуються в ПТК ЦСК Банку, функціонують на робочих станціях клієнтів (в тому числі і «тонкі» клієнти), що входять до складу автоматизованих робочих місць відповідальних осіб ЦСК Банку.

3.6. Резервування серверних застосувань ЦСК

Все серверне ПЗ функціонує на віртуальних серверах у віртуальній інфраструктурі основного і резервного ЦОД Банку. Віртуальна інфраструктура у кожному ЦОД має декілька систем зберігання даних та обчислювальних вузлів, які створюють відмово стійкий кластер.

Переключення ЦСК між ЦОД, для обслуговування клієнтів, відбувається за відповідним регламентом Банку.

Зокрема, резервування даних відбувається системою резервного копіювання відповідно до регламенту резервного копіювання.

3.7. Резервування спеціалізованих і неспеціалізованих робочих місць посадових осіб ЦСК

Всі робочі місця посадових осіб мають основне робоче місце на РС, що розгорнута за основним місцем роботи, та у віртуальному середовищі банку, що дозволяє виконувати свої обов'язки безпосередньо з резервного робочого місця.

3.8. Сервер застосувань ЦСК

Основними функціями серверу застосувань ЦСК є:

- управління ключами посадових осіб ЦСК (через спеціальне ПЗ, що встановлене на робочому місці адміністратора безпеки);
- управління ключами ЦСК (через спеціальне ПЗ, що встановлене на робочому місці адміністратора сертифікації);
- ведення БД сертифікатів, та запитів на формування сертифікату, запитів на блокування, поновлення і скасування сертифікатів (через відповідні клієнтські бібліотеки для роботи з БД);
- створення резервних копій БД серверу застосувань ЦСК Банку;
- відновлення БД після збоїв;
- формування, блокування, скасування та поновлення сертифікатів підписувачів, сервісу OCSP Банку (через обробку відповідних запитів з застосуванням ПЗ, що встановлене на робочому місці адміністратора сертифікації);
- формування запиту до ЗЦ НБУ на формування сертифікату сервісу TSP та управління його статусом (через обробку відповідних запитів з застосуванням ПЗ, що встановлене на робочому місці адміністратора сертифікації);
- формування СВС ключів;
- поширення сертифікатів підписувачів через поштові повідомлення та публікацію у LDAP-каталозі (через відповідні клієнтські бібліотеки для роботи з поштовим сервером та LDAP-каталогом);
- поширення СВС ключів підписувачів через поштові повідомлення та публікацію у LDAP-каталозі (через відповідні клієнтські бібліотеки для роботи з поштовим сервером та LDAP-каталогом);
- ідентифікація, автентифікація та авторизація відповідальних осіб ЦСК Банку (при підключенні спеціального ПЗ адміністраторів безпеки і сертифікації);
- ведення журналів аудиту функціонування серверу ЦСК;
- збереження особистого ключа ЦСК у захищеному вигляді.

3.9. Сервер надання послуг інтерактивного визначення статусу сертифікату

Сервер надання послуг інтерактивного визначення статусу сертифікату – OCSP-сервер, отримує від клієнтського програмного забезпечення – бібліотеки високорівневих криптографічних функцій запиту, за яким OCSP-сервер робить пошук у СВС вказаного сертифікату. Якщо сертифікат присутній у СВС, то у відповідь клієнт отримує відповідь, підписану ЕЦП OCSP-сервера, що сертифікат блоковано, поновлено, скасовано і т.д.

3.10. Сервер надання послуги фіксування часу

Сервер надання послуг фіксування часу – TSP-сервер, отримує від клієнтського програмного забезпечення – бібліотеки високорівневих криптографічних функцій, запит з хеш-образом документу, за яким TSP-сервер робить фіксування моменту часу та у відповідь надсилає підписану ЕЦП позначку часу та хеш-образ документу.

3.11. Клієнтські застосування

З використання клієнтських застосувань ініціюється:

- виконання технічних і технологічних функцій ПТК ЦСК з використанням серверних застосувань;
- генерування і зберігання особистих і відкритих ключів ЦСК банку та відповідальних осіб ЦСК банку за допомогою надійних засобів ЕЦП, що мають позитивний експертний висновок Держспецзв'язку;
- вивантаження власних відкритих ключів ЦСК банку для засвідчення їх чинності в ЗЦ НБУ;
- вивантаження відкритих ключів OCSP, TSP та відкритих ключів відповідальних осіб ЦСК банку для засвідчення їх чинності у ЦСК банку.

3.11. Обмеження на порядок доступу до серверних застосувань та БД

Лише за допомогою серверних застосувань може проводитися завантаження/вивантаження інформації в/із БД шляхом використання клієнтського застосування системи керування БД.

Клієнтські застосування, що функціонують у складі автоматизованих робочих місць, отримують доступ до інформації в БД за допомогою серверних застосувань.

3.12. Моніторинг і діагностика роботи ПТК ЦСК

Для забезпечення надійності і безперервності роботи всіх компонентів ПТК ЦСК, розгорнуто АРМ системного адміністратору ЦСК.

Результати моніторингу та перевірки діагностики всіх компонентів ПТК ЦСК ведуться у локальній БД АРМ системного адміністратора, який забезпечує цілісність і авторство даних.

4. РЕЖИМИ ДОСТУПУ ДО ІНФОРМАЦІЇ В ЦСК

4.1. Види інформації

У ЦСК 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 «конфіденційно».

4.2. 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 ЦСК і розсилання засобами електронної пошти (e-mail) банку.

До відкритої інформації ЦСК інформації, яка потребує захисту (забезпечення цілісності та доступності), належать:

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

4.3. Інформація з обмеженим доступом у електронній формі

До інформації з обмеженим доступом ЦСК у електронній формі належать:

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

4.4. Інформація з обмеженим доступом у паперовій формі

До інформації з обмеженим доступом ЦСК у паперовій формі належать документи:

- що подаються до ЦСК під час проведення процедур реєстрації, формування сертифікатів, зміни статусу сертифікатів, зміни ідентифікаційних даних підписувачів і не підлягають безпосередньому оприлюдненню;
- журнали аудиту (журнали обліку КСЗІ, обліку носіїв інформації, проведення регламентних процедур, технічного обслуговування ПТК ЦСК);
- інструкції відповідальних осіб ЦСК банку;
- інструкції щодо роботи з ключовими даними.

4.5. Доступ до інформації з обмеженим доступом

Доступ до інформації з обмеженим доступом ЦСК, мають відповідальні особи ЦСК банку з дотриманням вимог визначених політикою безпеки ЦСК.

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. Система захисту інформації ПТК ЦСК

Захист інформації в ПТК ЦСК забезпечується в результаті впровадження СЗІ. СЗІ ПТК ЦСК відповідає вимогам нормативно-правових актів законодавства України з питань захисту інформації.

5.2. Криптографічний захист інформації ПТК ЦСК

Усі засоби криптографічного захисту інформації ПТК ЦСК мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

5.3. Носії ключової інформації

У ПТК ЦСК використовуються такі НКІ:

- захищений файловий контейнер, що може зберігатися на НГМД, НЖМД, НЖМОД, flash-накопичувачі, CD чи DVD дисках;
- захищених апаратних носіях, що реалізують інтерфейс PKCS#11:

5.4. Вимоги до носіїв ключової інформації

Захищені НКІ, що використовуються в ПТК ЦСК, відповідають таким вимогам:

- робота з НКІ можлива лише після введення правильного пароля доступу;
- неможливість дублювання кожного з екземплярів НКІ;
- під час виконання криптографічних операцій ключова інформація та результати проміжних розрахунків захищені від стороннього доступу;
- захист особистих ключів передбачено шляхом забезпечення неможливості доступу до них у разі не знання пароля доступу;
- після введення помилкового паролю три рази, носій блокується і не дозволяє у подальшому виконувати доступ до нього;
- має засоби захисту критичної інформації, яка міститься в НКІ, від сучасних типів атак, побудованих на аналізі параметрів НКІ, які доступні для вимірювання ззовні під час роботи цієї апаратури;
- мають позитивний експертний висновок Держспецзв'язку.

5.5. Інформація, що міститься на НКІ

На захищених НКІ сервісу OCSP, TSP, відповідальних осіб ЦСК і підписувачів містяться такі дані:

- поточний особистий ключ ЕЦП сервісу OCSP, TSP, відповідальних осіб ЦСК чи підписувача;
- поточний сертифікат ЕЦП та запит на формування сертифікату майбутнього відкритого ключа (у разі наявності);
- поточний сертифікат ЕЦП власного відкритого ключа ЦСК;
- поточний особистий ключ для вироблення спільного секрету сервісу OCSP, TSP, відповідальних осіб ЦСК чи підписувача;
- поточний сертифікат вироблення спільного секрету та запит на формування майбутнього сертифікату (у разі наявності).

5.6. Доступ до приміщень

Серверне обладнання ПТК ЦСК розміщується у ЦОД. Усі автоматизовані робочі місця ЦСК розміщуються в приміщеннях з обмеженим доступом за адресами:

- Україна, м Львів, вул. Луганська, 16.
- Україна, м Львів, вул. Сахарова, 78А.

АРМ операторів реєстрації розташовуються в контрольованій зоні приміщень відділень банку.

5.7. Вимоги до серверних приміщень

ЦОД та приміщення з обмеженим доступом відповідають вимогам Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджених постановою Правління Національного банку України від 04.07.2007 №243.

"Правила з організації захисту приміщень банків України", затверджені Постановою Національного банку України N 195-ДСК від 04.06.2013р.

5.8. Відповідальність за збереження НКІ

Відповідальні особи ЦСК повинні зберігати НКІ зі своїми криптографічними ключами у сейфах/ящиках/шафах, що надійно замикаються, до яких не мають доступу сторонні особи, і несуть особисту відповідальність за надійне зберігання НКІ та нерозголошення паролів доступу і розблокування. Відповідальні особи ЦСК повинні зберігати основний пристрій НКІ на своєму основному робочому місці, а резервний пристрій НКІ – на резервному робочому місці.

Адміністратор сертифікації ЦСК повинен зберігати основні та частину резервних НКІ з ключами ЦСК у сейфі на своєму основному робочому місці, іншу частину резервних НКІ з

ключами ЦСК – на резервному робочому місці. Він несе особисту відповідальність за надійне зберігання цих НКІ та нерозголошення значень паролів доступу і розблокування.

Адміністратор сертифікації ЦСК повинен забезпечити зберігання резервних копій реєстру ЦСК у сейфах на своїх основному та резервному робочих місцях.

5.9. Особливості збереження ключових даних

Підсистема управління ключами забезпечує збереження наступних ключових даних:

- кореневий сертифікат;
- особисті ключ ЕЦП ЦСК;
- особисті ключі ЕЦП посадових осіб ЦСК;
- особисті ключі ЕЦП користувачів;
- особисті ключі вироблення спільного секрету користувачів;
- довгострокові ключові елементи, які використовуються для шифрування (за наявності).

Перераховані ключові дані зберігаються у складі ключового (файлового НКІ або на захищеному апаратному НКІ) контейнера виключно в зашифрованому виді. Шифрування виконується відповідно до ДСТУ ГОСТ 28147: 2009 в режимі простої заміни.

5.11. Особливості збереження особистого ключа ЦСК

Шифрування даних підпису власного особистого ключа ЕЦП ЦСК виконується за допомогою спеціального секретного ключа шифрування даних, який розподіляється між трьома і більше посадовцями ЦСК. Порядок розподілу цього ключа забезпечує:

- жоден посадовець одноосібно не може забезпечити розшифровування особистого ключа ЕЦП ЦСК;
- особистий ключ ЕЦП ЦСК може бути розшифрований тільки за умови пред'явлення будь-кими двома з посадовців частин спеціального секретного ключа, що належать їм.

5.12. Особливості збереження особистого ключа відповідальної особи ЦСК

Захист особистого ключа відповідальної особи ЦСК (адміністратора безпеки ЦСК, адміністратора сертифікації, адміністратора реєстрації) забезпечується за допомогою симетричного криптографічного перетворення за ГОСТ 28147-89, з використанням ключа, який виробляється на основі особистого пароля цього посадовця. Формування секретного ключа виконується шляхом хешування особистого пароля за ГОСТ 34.311-95.

5.13. Особливості збереження особистого ключа підписувача

Шифрування даних особистого ключа користувача забезпечується за допомогою ключа, який виробляється на основі особистого пароля користувача. Створення секретного ключа виконується шляхом хешування особистого пароля користувача за ГОСТ 34.311-95.

5.14. Зберігання НКІ

Зберігання особистих ключів відповідальних осіб ЦСК і користувачів виконується виключно на носіях, що належать їм, і тільки в зашифрованому виді. Будь-які інші варіанти збереження вказаних особистих ключів виключені.

5.15. Обов'язкові можливості серверних застосувань та автоматизованих робочих місць

Серверні застосування та всі автоматизовані робочі місця 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.

5.16. Захист персональних даних підписувачів

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 технічні заходів, реалізованих у результаті впровадження СЗІ, у тому числі: використання надійних засобів ЕЦП, ведення журналів роботи системи в захищеному вигляді, розмежування та здійснення контролю за інформаційними потоками між внутрішньою локальною мережею ЦСК і підсистемою відкритого доступу, використання антивірусних засобів, міжмережевих екранів тощо.

6. ЖУРНАЛИ АУДИТУ ПТК ЦСК

6.1. Перелік журналів аудиту

У ПТК ЦСК ведуться такі журнали аудиту:

- журнали обліку НКІ;
- журнали видачі НКІ підписувачам і посадовим особам ЦСК;
- журнал обліку подій генерації ключів;
- журнал резервного копіювання;
- журнал обліку подій збоїв та відмов ПТК ЦСК;
- журнал обліку носіїв конфіденційної інформації.

Журнали функціонування ПЗ та НКІ в ПТК ЦСК ведуться в електронній формі на всіх серверних і клієнтських застосуваннях. Інші журнали ведуться на паперових носіях.

6.2. Вимоги до журналів аудиту у електронній формі

ПЗ ПТК ЦСК забезпечує захищене від модифікації протоколювання подій, пов'язаних з функціонуванням ПЗ та НКІ. Захист від модифікації забезпечується встановленням правил розмежування доступу засобами ОС та накладанням ЕЦП чи кодів автентифікації для записів у журналі. Ці журнали подій містять дату та час події, опис події. У журналі реєструються події, пов'язані з:

- генеруванням, резервуванням, використанням і знищенням особистих ключів ЦСК, відповідальних осіб ЦСК та підписувачів;
- формуванням, переформуванням, зміною статусу сертифікатів сервісу OCSP, TSP, відповідальних осіб ЦСК і підписувачів;
- унесенням, модифікацією та видаленням даних про сервіси OCSP, TSP, відповідальних осіб ЦСК і підписувачів.

6.3. Ведення журналу видачі НКІ посадовим особам ЦСК

Служба захисту інформації ЦСК веде журнал подій, пов'язаних з видачею НКІ, які використовуються відповідальними особами ЦСК. Цей журнал подій містить дату та час події, опис події, серійний номер НКІ, підпис відповідальної особи ЦСК, яка отримує НКІ від адміністратора безпеки ЦСК чи передає йому свій НКІ, підпис адміністратора безпеки ЦСК. У журналі реєструються події, пов'язані з видачею/поверненням НКІ відповідальними особами ЦСК.

6.4. Ведення журналу видачі НКІ підписувачів

Служба реєстрації ЦСК веде журнал подій, пов'язаних з видачею НКІ підписувачам. Цей журнал подій містить дату та час події, опис події, серійний номер НКІ, підпис заявника

(підписувача - працівника банку), який отримує НКІ від адміністратора реєстрації ЦСК, підпис адміністратора реєстрації ЦСК. У журналі реєструються події, пов'язані з видачею НКІ підписувачам.

6.5. Ведення журналу обліку НКІ

В ЦСК ведеться журнал обліку захищених НКІ, які облікуються ЦСК. Цей журнал подій містить дату та час події, опис події, серійні номери НКІ, підпис отримувача (працівника банку).

6.6. Ведення журналу обліку подій генерації ключів

В ЦСК ведеться журнал подій, пов'язаних з операціями над ключами підписувачів, технологічних серверів та ключів ЦСК. Цей журнал подій містить дату події, тип НКІ та ідентифікаційні дані, опис події, підпис посадової особи, що проводила операції, які не ведуться у електронному вигляді. У паперовому журналі реєструються події, пов'язані з:

- прийманням заяв про формування, зміну статусу сертифіката підписувача, про внесення змін до ідентифікаційних даних підписувача;
- унесенням підписувачів до реєстру ЦСК (генерація ключів.).

6.7. Ведення журналу реєстрації збоїв та відмов ПТК ЦСК

Системний адміністратор веде журнал реєстрації збоїв та відмов ПТК ЦСК. Цей журнал містить дату та час події, її опис, підпис системного адміністратора, резолюція начальника ЦСК, опис робіт з усунення збоїв і відмов. У журналі реєструються події, пов'язані з:

- відмовою чи збоями у роботі компонентів ПТК ЦСК;
- описом робіт, які проведені для усунення недоліків.

6.8. Ведення журналу резервного копіювання

Системний адміністратор веде журнал резервного копіювання даних ПТК ЦСК. Цей журнал містить дату та час події, її опис, підпис системного адміністратора, серійний номер носія інформації куди записана резервна копія. У журналі реєструються події, пов'язані з резервним копіюванням критичних даних відповідно до регламенту резервного копіювання.

6.9. Ведення журналу обліку носіїв конфіденціальної інформації

Служба захисту інформації ЦСК веде журнал обліку всіх типів носіїв, які призначені для зберігання конфіденційної інформації ЦСК, які використовуються відповідальними особами ЦСК. Цей журнал містить найменування носія, реєстраційний номер, звідки надійшов, або ким створений, куди надіслано або переданий, номер акту про знищення. У журналі реєструються події, пов'язані з отриманням/передачею носіїв відповідальними особами ЦСК.

6.10. Відповідальність за збереження журналів аудиту

Журнали аудиту роботи ПТК ЦСК та НКІ ведуться на відповідних серверах та робочих місцях відповідальних осіб ЦСК.

Відповідальні особи ЦСК здійснюють на своїх автоматизованих робочих місцях резервне копіювання журналів функціонування ПЗ та НКІ в ПТК ЦСК шляхом їх запису на знімні носії.

Відповідальні особи ЦСК зберігають ці копії журналів у сейфах сейфах/ящиках/шафах, що надійно замикаються і до яких не мають доступу сторонні особи.

6.11. Доступ до журналів аудиту

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

Адміністратор безпеки ЦСК забезпечує за зверненням відповідальних осіб ЦСК перегляд журналів аудиту, що ведуться:

- серверними застосуваннями;
- клієнтськими застосуваннями на інших автоматизованих робочих місцях;
- іншими відповідальними особами ЦСК.

6.12. Строк зберігання журналів аудиту

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

7. ОСОБИСТІ КЛЮЧІ В ЦСК

7.7. Генерація і резервування ключів ЦСК та відповідальних осіб ЦСК

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

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

7.2. Збереження ключів ЦСК та відповідальних осіб ЦСК

Особисті ключі ЦСК, зберігаються виключно у вигляді спеціального файлового ключового контейнеру, який зашифрований за допомогою секретного ключа шифрування ДСТУ ГОСТ 28147-89, розподілений між всіма відповідальними особами, що приймали участь у процедурі генерації ключів ЦСК. Методика зберігання особистих ключів ЦСК узгоджена з Держспецзв'язком.

Відповідальні особи ЦСК, зберігають свої особисті ключі виключно на захищених НКІ.

7.3. Строк чинності особистого ключа ЦСК

Строк чинності особистого ключа дорівнює строку чинності відповідного сертифіката. Особистий ключ тимчасово не є чинним у разі блокування відповідного сертифіката. Строк чинності сертифікату ЦСК складає 2 роки.

7.4. Види криптографічних алгоритмів, ключі та їх довжини

У ЦСК генеруються та використовуються такі криптографічні ключі:

- власні (особистий та відкритий) ключі ЦСК для криптографічного алгоритму ДСТУ 4145-2002 (довжина 257 біт);
- особистий та відкритий ключі ЦСК послуги визначення статусу сертифіката для криптографічного алгоритму ДСТУ 4145-2002 (довжина 257 біт);
- особистий та відкритий ключі ЦСК послуги надання позначки часу для криптографічного алгоритму ДСТУ 4145-2002 (довжина 257 біт);
- особистий та відкритий ключі відповідальних осіб та підписувачів ЦСК для криптографічного алгоритму ДСТУ 4145-2002 (довжина 257 біт).
- особистий та відкритий ключі відповідальних осіб та підписувачів ЦСК для криптографічного протоколу Діфі-Хелмана відповідно до наказу Держспецзв'язку від 18.12.2012 №739 «Про затвердження Вимог до форматів криптографічних повідомлень» (довжина 257 біт).

7.5. Генерація ключів підписувачами

Відповідальні особи ЦСК забезпечують підписувача надійними криптографічними засобами та надає йому допомогу під час генерування ключів у разі потреби.

7.6. Область застосування особистих ключів ЦСК

Особисті ключі ЦСК використовуються виключно для формування СВС, сертифікатів сервісу OCSP, TSP, відповідальних осіб ЦСК, технологічних серверів банківських систем та систем електронного документообігу, підписувачів.

Особисті ключі послуги надання позначки часу використовуються виключно під час формування відповіді на запит на позначку часу.

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

Особисті ключі відповідальних осіб ЦСК використовуються виключно для їх автентифікації в ПТК ЦСК та перевірки цілісності даних, які обробляються відповідальними особами ЦСК.

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 підписувача на його вимогу.

7.8. Компрометація особистих ключів ЦСК та особистих ключів послуги фіксування часу

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

Служба сертифікації ЦСК у разі компрометації або загрози компрометації особистих ключів ЦСК та особистих ключів TSP:

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

7.9. Компрометація особистих ключів послуги інтерактивного визначення статусу сертифіката

Служба сертифікації ЦСК у разі компрометації або загрози компрометації особистих ключів сервісу OCSP:

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

7.10. Компрометація особистих ключів відповідальної особи ЦСК

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

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

Відповідальна особа ЦСК негайно змінює пароль доступу до НКІ в разі компрометації чи

загрози компрометації пароля доступу.

7.11. Знищення особистих ключів

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

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. Ведення реєстру сертифікатів

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

8.2. Формат сертифікатів

ЦСК формує сертифікати відповідно до Вимог до формату посиленого сертифіката, затверджених наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453, зареєстрованих у Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710 (зі змінами).

8.4. Формування сертифікатів в ЦСК

Служба сертифікації ЦСК формує сертифікати OCSP, відповідальних осіб ЦСК та підписувачів.

8.5. Область використання сертифікатів відкритих ключів ЦСК

Сертифікати відкритих ключів ЦСК використовуються виключно для перевірки СВС, сертифікатів OCSP, відповідальних осіб ЦСК та підписувачів.

8.6. Область використання сертифікатів відкритих ключів OCSP

Сертифікати OCSP використовуються виключно для перевірки ЕЦП під час надання послуг інтерактивного визначення статусу сертифікатів.

8.7. Область використання сертифікатів відкритих ключів TSP

Сертифікати TSP використовуються виключно для перевірки ЕЦП під час надання послуг надання позначки часу.

8.8. Область використання сертифікатів відкритих ключів відповідальних осіб ЦСК

Сертифікати відповідальних осіб ЦСК використовуються виключно для ідентифікації та автентифікації відповідальних осіб ЦСК під час завантаження їх автоматизованих робочих місць та перевірки ЕЦП, що накладаються ними на документи під час виконання своїх функціональних обов'язків.

8.9. Область використання сертифікатів відкритих ключів підписувачів

Сертифікати, сформовані в ЦСК для Підписувачів, використовуються для підтвердження ЕЦП. ЦСК під час формування сертифікатів підписувачів зазначає сфери використання цих сертифікатів та обмеження щодо їх використання.

8.10. Строк чинності сертифікатів ЦСК

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

8.11. Строк чинності сертифікатів відповідальних осіб ЦСК

Строк чинності сертифікатів відповідальних осіб ЦСК становить один рік після чого проводиться їх планова заміна згідно з вимогами цього Регламенту.

8.12. Строк чинності сертифікатів підписувачів

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

8.13. Блокування і скасування сертифікатів

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

8.14. Зберігання сертифікатів відповідальних осіб ЦСК

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

9. ПОРЯДОК ПОДАННЯ ДОКУМЕНТІВ ПІД ЧАС ПРОВЕДЕННЯ РЕГЛАМЕНТНИХ ПРОЦЕДУР

9.1. Звернення підписувачів

Заявник особисто подає до ЦСК заяви, див. додаток А, (ЦСК самостійно розробляє форми заяв, скарг, довіреностей – фізичні особи, ФОП, юридичні особи) про реєстрацію, формування сертифікату, зміну статусу сертифіката підписувача, унесення змін до ідентифікаційних даних підписувача, договір на підставі якого підписувачу, який є клієнтом банку, надаються послуги ЕЦП, у паперовій та/чи електронній формі.

9.2. Звернення підписувачів, що є працівниками банку

Підписувач, який є працівником банку, особисто подає до ЦСК заяви, див. Додаток Б, (ЦСК самостійно розробляє форми заяв) про реєстрацію, формування сертифікату, зміну статусу сертифіката, унесення змін до своїх ідентифікаційних даних у паперовій та/чи електронній формі.

9.3. Засвідчення чинності звернення

Адміністратор реєстрації ЦСК засвідчує подані в електронному вигляді заяви шляхом накладання на них ЕЦП.

9.4. Заява про формування сертифікату

У заяві про формування сертифікату повинні зазначатися:

- ідентифікаційні дані підписувача;
- ідентифікаційні дані заявника (для підписувача, який є клієнтом банку);
- дані, що включаються до сертифікату підписувача.

На етапі генерації стартових ключів, оператором реєстрації, вводиться фраза-пароль для блокування стартового чи робочого сертифіката за телефоном. Адміністратор реєстрації також може ввести інформацію про фразу-пароль для блокування сертифіката телефоном, на етапі засвідчення запита на формування сертифікату робочого відкритого ключа.

9.5. Заява про зміну статусу сертифікату

У заяві про зміну статусу сертифіката повинні зазначатися:

- ідентифікаційні дані підписувача;
- ідентифікаційні дані заявника (для підписувача, який є клієнтом банку);
- реєстраційний номер сертифіката;

- підстави зміни статусу сертифіката.

9.6. Заява про внесення змін до ідентифікаційних даних

У заяві про внесення змін до ідентифікаційних даних підписувача повинні зазначатися:

- ідентифікаційні дані підписувача;
- ідентифікаційні дані заявника (для підписувача, який є клієнтом банку).

9.7. Прийом заяви

Заяви для здійснення регламентних процедур приймаються тільки за наявності всіх інших документів, визначених цим Регламентом для проведення відповідних процедур.

ЦСК не приймає на розгляд документи, які мають виправлення, дописки, закреслені слова, написи, а також пошкодження, унаслідок чого їх текст не можна прочитати.

9.8. Ідентифікація заявника

Адміністратор реєстрації ЦСК під час подання заяв про формування сертифікату, зміну статусу сертифіката підписувача та внесення змін до ідентифікаційних даних підписувача виконує процедуру ідентифікації (установлення особи) заявника (підписувача, який не є працівником Банку). Установлення особи заявника здійснюється за паспортом або іншими документами відповідно до законодавства України. Установлення особи підписувача, який є працівником Банку, здійснюється за його службовими документами (перепустка тощо).

9.9. Ідентифікація заявника за довіреністю

Заявник під час подання заяв, якщо заявник та підписувач, який є клієнтом банку, є різними суб'єктами, повинен подати до служби реєстрації ЦСК довіреність, яка засвідчується:

- для юридичних осіб - підписом керівника та відбитком печатки юридичної особи;
- для фізичних осіб-підприємців - підписом підприємця та відбитком його печатки або в разі відсутності печатки - нотаріально;
- для фізичних осіб - нотаріально.

У довіреності повинні зазначатися:

- ідентифікаційні дані підписувача, який є клієнтом банку;
- ідентифікаційні дані заявника;
- перелік регламентних процедур, які заявник може здійснювати від імені підписувача;
- дата початку та закінчення чинності довіреності.

9.10. Належність підписувача до юридичної особи

Заявник повинен додатково подати до ЦСК відомості щодо належності підписувача до юридичної особи, якщо підписувач є фізичною особою - представником юридичної особи.

10. ПОРЯДОК ОПРАЦЮВАННЯ ДОКУМЕНТІВ, ЩО ПОДАЮТЬСЯ ДО ЦСК ПІД ЧАС ПРОВЕДЕННЯ РЕГЛАМЕНТНИХ ПРОЦЕДУР

10.1. Взяття на облік заявника

Служба реєстрації ЦСК бере на облік усі документи, що були подані заявником під час проведення всіх регламентних процедур, шляхом формування справи підписувача та введення необхідних даних підписувачів у реєстр ЦСК. Справа підписувача реєструється в журналі, який ведеться в паперовому та електронному вигляді.

10.2. Перевірка повноти та відповідності наданих документів

Служба реєстрації ЦСК перевіряє повноту комплекту поданих для проведення відповідної

регламентної процедури документів, правильність їх оформлення і відповідність вимогам нормативних документів у сфері ЕЦП.

10.3. Відмова у проведенні регламентної процедури

Служба реєстрації ЦСК за результатом розгляду поданих документів приймає рішення про відмову в проведенні відповідної регламентної процедури, якщо:

- немає всіх необхідних для проведення цієї регламентної процедури документів;
- подано хоча б одну неналежно засвідчену копію документа;
- установлено невідповідність даних, що визначені поданими документами, фактичним;
- виявлено інші невідповідності законодавству України у сфері ЕЦП.

Служба реєстрації ЦСК повертає документи в разі відмови в проведенні відповідної регламентної процедури із зазначенням підстав відмови на цій заяві.

10.4. Перелік та форма документів, що подаються Заявником

Заявник (підписувач, який є працівником Банку) подає до ЦСК такі документи:

- засвідчені копії документів на паперовому носії;
- оригінали документів на паперовому носії (з необхідними підписами та відбитками печаток) і електронні варіанти цих документів.

10.5. Робота з засвідченими копіями документів на паперових носіях

Служба реєстрації ЦСК під час подання засвідченої копії документа на паперовому носії здійснює:

- переведення засвідченої копії документа на паперовому носії в електронний вигляд шляхом сканування;
- підшивання копії документа на паперовому носії до справи;
- накладення на електронний варіант відсканованої копії документа ЕЦП оператора реєстрації ЦСК засобами ПТК ЦСК;
- унесення до БД електронного варіанта відсканованої копії документа з ЕЦП оператора реєстрації ЦСК, що є дійсним на момент накладення ЕЦП.

10.6. Робота з оригіналами документів на паперових носіях

Служба реєстрації ЦСК під час подання оригіналу документа на паперовому (з необхідними підписами та печатками) та електронному носіях здійснює:

- перевірку чи електронний варіант документа підписано поточним та майбутнім (у разі наявності) особистими ключами підписувача. Разом з документом повинні подаватися сертифікати підписувача (у разі наявності) чи відкриті ключі, за допомогою яких можна перевірити ЕЦП підписувача;
- накладення ЕЦП оператора реєстрації ЦСК на електронний варіант документа засобами ПТК ЦСК;
- переведення оригіналу документа на паперовому носії в електронний вигляд шляхом сканування;
- підшивання оригіналу документа на паперовому носії до справи;
- накладення ЕЦП оператора реєстрації ЦСК на електронний варіант відсканованого оригіналу документа засобами ПТК ЦСК;
- унесення до БД електронного документа, ЕЦП ЦСК на електронний документ, ЕЦП оператора реєстрації ЦСК на електронний документ, електронного варіанта відсканованого оригіналу, ЕЦП оператора реєстрації ЦСК на електронний варіант відсканованого оригіналу, сертифікат оператора реєстрації ЦСК.

Служба реєстрації ЦСК проводить порівняння ідентифікаційних даних підписувача у заяві

про формування чи зміну статусу сертифіката підписувача з даними, одержаними під час реєстрації підписувача.

Служба реєстрації ЦСК проводить порівняння ідентифікаційних даних підписувача, наведених у заявах про формування сертифікату підписувача і про внесення змін до ідентифікаційних даних підписувача, з даними, що містяться в копіях документів, які підтверджують ці зміни, якщо формування нового сертифіката відбувається у зв'язку зі зміною ідентифікаційних даних підписувача, які внесені до реєстру ЦСК.

Якщо заявником подано оригінал документа, то копія такого документа може бути засвідчена підписом та відбитком печатки оператора реєстрації ЦСК.

11. РЕЄСТРАЦІЯ ПІДПИСУВАЧІВ

11.1. Умови обслуговування сертифікатів

Підписувач перед початком процедури реєстрації повинен ознайомитися з умовами обслуговування сертифікатів, передбачених політикою сертифікації ЦСК, зокрема з питаннями щодо:

- зобов'язань та підстав відповідальності ЦСК стосовно обслуговування сертифікатів;
- зобов'язань та підстав відповідальності підписувача стосовно використання сертифіката і зберігання особистого ключа;
- сфери використання підписувачем сертифіката;
- строків зберігання в ЦСК даних про підписувачів та заявників, що були отримані ЦСК під час реєстрації;
- відомостей про засоби ЕЦП, що можуть використовуватися для формування та перевірки ЕЦП.

11.2. Реєстрація підписувача

Заявник для проведення реєстрації підписувача в ЦСК (крім підписувача, який є працівником банку) надає оператору реєстрації ЦСК договір, на підставі якого підписувачу, який є клієнтом банку, надаються послуги ЕЦП.

Підписувач, який є працівником Банку, для проведення реєстрації підписує зобов'язання про дотримання умов використання ЕЦП.

11.3. Реєстрація підписувача – юридичної особи

Заявник юридичної особи під час проведення реєстрації в ЦСК подає такі документи:

- заповнену заяву про формування сертифікату, підписану керівником юридичної особи, засвідчену відбитком печатки юридичної особи;
- копії паспортів та довідок про присвоєння ідентифікаційного коду керівника та головного бухгалтера, засвідчені власноручними підписами власників паспортів (якщо сертифікати формуються для керівника та бухгалтера).

11.4. Реєстрація підписувача – відокремленого підрозділу юридичної особи

Заявник відокремленого підрозділу (філії, представництва) юридичної особи подає для реєстрації в ЦСК такі документи:

- заповнену заяву про формування сертифікату підписувача, підписану керівником відокремленого підрозділу, засвідчену відбитком печатки відокремленого підрозділу;
- копії паспортів та довідок про присвоєння ідентифікаційного коду керівника та головного бухгалтера відокремленого підрозділу, засвідчені власноручними підписами власників паспортів (якщо сертифікати формуються для керівника та бухгалтера).

11.5. Реєстрація підписувала – фізичної особи - суб'єкта підприємницької діяльності

Заявник фізичної особи - суб'єкта підприємницької діяльності подає для реєстрації в ЦСК заповнену заяву про формування сертифікату підписувача, підписану фізичною особою - суб'єктом підприємницької діяльності, заявником та засвідчену відбитком печатки фізичної особи - суб'єкта підприємницької діяльності (у разі наявності печатки).

11.6. Особливості реєстрації працівників банку

Підписувач, який є працівником банку, для реєстрації подає заповнену заяву про формування сертифікату, підписану ним особисто та оригіналу (завірену копію) наказу про призначення на посаду.

11.7. Процедура реєстрації

11.7.1. Процедура реєстрації підписувача ДБО

Первинна реєстрація заявника, як майбутнього (потенційного) клієнта ДБО здійснюється в такому порядку.

1. Заявник відвідує відділення банку (ВПР) для подання зазначених вище документів, та формування стартової ключової пари, строк дії якої обмежений 14 днями з моменту підписання договору на обслуговування. Стартова ключова пара може бути збережена у вигляді файлового ключового контейнера чи записана на захищений НКІ. Після зазначеного строку створення запиту на формування сертифікату буде неможливе, підписувач повинен повторно відвідати ВПР для отримання стартової ключової пари.

2. Заявник заходить з свого робочого місця на web-сторінку ДБО для заповнення реєстраційної форми користувача ДБО, ознайомлюється з вимогами, обв'язками та правами користувача ДБО. Для входу до ДБО, використовується стартова ключова пара, яка автоматично змінюється – генерується робоча ключова пара, яка зберігається у НКІ та формується PKCS#7 запит на формування сертифікату підписувача, який засобами ДБО передається до Служби реєстрації ЦСК банку.

ЦСК під час подання зазначених вище документів оператор реєстрації проводить їх реєстрацію в такому порядку.

а) Служба реєстрації ЦСК опрацьовує подані документи протягом 1 робочого дня з моменту їх надходження згідно з вимогами цього Регламенту.

б) Служба реєстрації ЦСК у разі наявності всіх необхідних правильно оформлених документів підтверджує запит на формування сертифікату, а також уносить до реєстру ЦСК необхідні дані підписувача згідно з вимогами цього Регламенту.

в) Заявник під час проведення реєстрації в ЦСК подає запит на формування сертифікату підписувача через форму реєстрації користувачі ДБО (описано вище) зі свого робочого місця або генерує запит на формування сертифікату підписувача в ЦСК на робочій станції генерування ключів підписувачів.

г) Служба сертифікації ЦСК формує сертифікат підписувача згідно з вимогами цього Регламенту та поширює його в порядку, визначеному цим Регламентом.

д) Підписувач на своєму робочомі місці авторизується у системі ДБО за допомогою контейнеру своїх ключів і засобами ДБО завантажує опублікований сертифікат підписувача та записує його до ключового контейнера.

Служба реєстрації ЦСК після завершення процедури реєстрації надає заявнику для підписувача юридичної особи чи підписувача фізичної особи – підприємця, за потреби захищений НКІ та відповідне ПЗ.

11.8.2. Процедура реєстрації підписувача співробітника банку

ЦСК під час подання зазначених вище документів проводить їх реєстрацію в такому порядку.

1. Співробітник Банку звертається до оператора реєстрації у відокремленому підрозділі Банку та надає документи для формування запиту на формування сертифікату.

2. Служба реєстрації ЦСК опрацьовує подані документи протягом однієї години з моменту їх надходження згідно з вимогами цього Регламенту.

3. Служба реєстрації ЦСК у разі наявності всіх необхідних правильно оформлених документів формує стартові ключі з стартовим сертифікатом на захищеному НКІ, а також уносить до реєстру ЦСК необхідні дані підписувача згідно з вимогами цього Регламенту.

4. Заявник авторизується зі свого робочого місця до автоматизованої системи. Під час автентифікації, автоматизована система визначає, що підписувачем використовуються стартові ключі, які необхідно змінити на робочі. Підписувачу обов'язково пропонується змінити пароль доступа до ключового контейнеру, у випадку користування файловим контейнером, та генерується робоча ключова пара, яка зберігається у файловому ключовому контейнері та формується PKCS#7 запит на формування сертифікату підписувача, який засобами автоматизованої системи передається до Служби реєстрації ЦСК Банку.

5. Служба реєстрації ЦСК уносить запит на формування сертифікату підписувача до реєстру ЦСК.

6. Служба сертифікації ЦСК формує сертифікат підписувача згідно з вимогами цього Регламенту та поширює його в порядку, визначеному цим Регламентом.

7. Підписувач через деякий час повторно авторизується у автоматизованій системі і завантажує опублікований сертифікат підписувача та записує його до ключового контейнера.

11.9. Скасування процедури реєстрації

ЦСК скасовує реєстрацію підписувача в разі:

- подання заявником заяви про скасування реєстрації підписувача;
- невиконання підписувачем, який є клієнтом банку, умов договору, на підставі якого йому надаються послуги ЕЦП;
- звільнення з роботи підписувача, який є працівником юридичної чи фізичної особи;
- звільнення з роботи підписувача, який є працівником банку;
- отримання наказу про скасування реєстрації підписувача, який є працівником банку;
- наявності рішення суду про скасування реєстрації підписувача, що набрало законної сили.

11.10. Процедура скасування реєстрації

ЦСК здійснює скасування реєстрації підписувача в такому порядку:

- служба реєстрації ЦСК змінює статус зареєстрованого підписувача на скасований;
- служба сертифікації ЦСК формує запит на скасування сертифікату підписувача, на основі якого формується СВС. СВС поширюється в порядку, визначеному цим Регламентом;
- ЦСК письмово повідомляє підписувача про рішення щодо скасування його реєстрації із зазначенням підстав;
- ЦСК поширює інформацію про скасування реєстрації цього підписувача шляхом унесення відповідних змін до інформації на інформаційному ресурсі ЦСК.

12. ФОРМУВАННЯ УНІКАЛЬНОГО РОЗПІЗНАВАЛЬНОГО ІМЕНІ ПІДПИСУВАЧА

12.1. Забезпечення унікальності

Служба реєстрації ЦСК формує унікальне розпізнавальне ім'я підписувача під час унесення даних про нього до реєстру ЦСК. Забезпечення його унікальності відбувається шляхом додавання до розпізнавального імені підписувача реквізиту «серійний номер» (поле «SERIALNUMBER»).

12.2. Порядок формування серійного номеру

Значення реквізиту «серійний номер» для підписувача формується таким чином:

- UA-[код установи/особи] {-[додаток]},

де код установи/особи - 8, 9 або 10 цифр, що містять код за ЄДРПОУ організації юридичної особи, код ДРФО фізичної особи-підприємця, яка є суб'єктом підприємницької діяльності, за установчими документами або відомостями про державну реєстрацію або ідентифікаційний код фізичної особи;

додаток - необов'язкова послідовність від 1 до 4 цифр, що містить додаткову частину ідентифікатора. У разі використання додатка він відокремлюється від коду установи/особи символом «-».

13. ГЕНЕРУВАННЯ КРИПТОГРАФІЧНИХ КЛЮЧІВ ПІДПИСУВАЧА ТА ЗАПИТУ НА ФОРМУВАННЯ СЕРТИФІКАТУ

13.1. Місце генерації ключів підписувачів

Відкритий та особистий ключі підписувача можуть бути згенеровані:

- на робочому місці підписувача;
- у ЦСК на робочій станції генерування ключів підписувачів.

13.2. Генерація ключів

Для заявника юридичної особи чи фізичної особи-підприємця, можуть бути сформовані ключі за допомогою криптографічних засобів інформації вбудованих до засобів ДБО. Генерування криптографічних ключів та запитів на формування сертифікату підписувача можу бути виконано на його робочому місці. Ці засоби ЕЦП створюють запит у форматі, визначеному цим Регламентом.

Для співробітника Банку, можуть бути сформовані ключі за допомогою криптографічних засобів інформації вбудованих до засобів автоматизованої системи. Генерування криптографічних ключів та запитів на формування сертифікату підписувача можу бути виконано на його робочому місці. Ці засоби ЕЦП створюють запит у форматі, визначеному цим Регламентом.

13.3. Запити на формування сертифікату

Запит на формування сертифікату підписувача може бути двох видів:

- у форматі PKCS#10;
- у форматі PKCS#7 з накладеним ЕЦП з використанням особистого підписувача.

13.4. Передача права на генерацію ключів

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

13.5. Генерація ключів працівниками банку

Підписувач, який є працівником банку, отримує стартові ключі в оператора реєстрації та проводить зміну стартових ключів на робочі:

- на робочій станції генерування ключів, що входить до складу ПТК ЦСК;
- на своєму робочому місці.

13.6. Зберігання особистого ключа та відповідальність

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.

13.7. Знищення особистого ключа

ПТК ЦСК забезпечує знищення особистого ключа підписувача на робочій станції, на якій генерувалися ключі, методом, що не допускає можливості його відновлення, після генерування та запису ключів на НКІ.

13.8. Підтвердження факту генерації ключів

Заявник, якщо генерування ключів здійснювалося в ЦСК, вкладає НКІ та фразу-пароль у непрозорий конверт, який запечатується, засвідчується відбитком печатки ЦСК, підписами заявника та оператора реєстрації ЦСК.

13.9. Отримання особистих ключів від заявника

Підписувач під час отримання конверта з НКІ та фразою-паролем зобов'язаний перевірити цілісність цього конверта. Якщо цілісність не порушена, при першому використанні особистого ключа, підписувач зобов'язаний змінити пароль доступу до нього. Підписувач зобов'язаний терміново звернутися до ЦСК із заявою про скасування сертифіката відповідного особистого ключа, якщо цілісність конверта порушена.

14. ФОРМУВАННЯ СЕРТИФІКАТУ ПІДПИСУВАЧА

14.1. Підстава для формування сертифікату

ЦСК формує сертифікати підписувачів тільки під час проведення процедури реєстрації підписувача або для зареєстрованих підписувачів у разі подання підписувачем/заявником заяви про формування сертифікату підписувача.

14.2. Вихідні дані для сертифікату

ЦСК здійснює формування сертифікату підписувача на підставі даних, що містяться в запиті про формування сертифікату.

14.3. Термін розгляду заяви на формування сертифікату

Час розгляду заяви про формування сертифікату підписувача, зареєстрованого в ЦСК, становить не більше:

- для працівника банка до однієї години;
- для клієнту банка протягом одного робочого дня.

14.4. Процедура формування сертифікату

ЦСК здійснює формування сертифікатів підписувачів у такому порядку.

1. Служба реєстрації ЦСК опрацьовує поданий заявником запит на формування сертифікату підписувача та документи згідно з вимогами цього Регламенту і встановлює належність

підписувачу особистого ключа та його відповідність відкритому ключу.

2. Служба реєстрації ЦСК вносить поданий заявником запит про формування сертифікату підписувача до БД.

3. ЦСК приймає рішення про формування/відмову в формуванні сертифікату підписувача.

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

5. Служба сертифікації ЦСК формує сертифікати підписувача в разі позитивного рішення ЦСК.

6. Служба сертифікації ЦСК під час формування сертифікату підписувача:

- визначає дату і час початку та закінчення строку чинності сертифіката підписувача;
- уносить до сертифіката підписувача обов'язкові дані, визначені Законом України «Про електронний цифровий підпис»;
- уносить до сертифіката підписувача додаткові дані за зверненням заявника;
- уносить до сертифіката підписувача інформацію щодо місця розміщення СВС на інформаційному ресурсі ЦСК;
- забезпечує унікальність реєстраційного номера сертифіката в межах ЦСК, а також унікальність відкритих ключів у реєстрі чинних, блокованих та скасованих сертифікатів.

7. Служба сертифікації ЦСК під час формування нового сертифіката підписувача створює запит про скасування поточного сертифіката підписувача, засвідчує його, формує та поширює СВС і тільки після цього формує новий сертифікат підписувача.

8. Служба реєстрації ЦСК після формування сертифікату підписувача надає його заявнику. Заявник повинен перевірити правильність відомостей, що містяться в сертифікаті підписувача. У разі виявлення некоректних даних (помилки в реквізитах) він повинен повідомити про зазначене службу реєстрації ЦСК. У цьому разі сертифікат скасовується та формується новий сертифікат підписувача.

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

14.5. Використання попереднього особистого ключа для підписування запиту на формування наступного сертифікату відкритого ключа

Для заявника юридичної особи, фізичної особи-підприємця та фізичної особи, може бути проведено зміну ключа за допомогою криптографічних засобів інформації вбудованих до засобів ДБО. Зміна криптографічних ключів та формування запитів на формування сертифікату підписувача можу бути виконано на його робочому місці. Ці засоби ЕЦП створюють запит у форматі PKCS#7, визначеному цим Регламентом, підписаного за допомого особистого ключа ЕЦП, якщо відповідний йому особистий ключ не був скомпрометований або не закінчив строк дії. Запит на формування сертифікату доставляється до Служби реєстрації ЦСК засобами ДБО.

Для співробітника банку, може бути проведено зміну ключів за допомогою криптографічних засобів інформації вбудованих до засобів автоматизованої системи. Зміна криптографічних ключів та формування запитів на формування сертифікату підписувача можу бути виконано на його робочому місці. Ці засоби ЕЦП створюють запит у форматі PKCS#7, визначеному цим Регламентом, підписаного за допомого особистого ключа ЕЦП, якщо відповідний йому особистий ключ не був скомпрометований або не закінчив строк дії. Запит на формування сертифікату доставляється до Служби реєстрації ЦСК засобами автоматизованої системи.

Строк чинності особистого ключа підписувача не може перевищувати один рік.

14.6. Терміни подачі заяви на формування сертифікату

Заявник подає до ЦСК заяву про формування нового сертифіката підписувача не пізніше ніж за десять робочих днів (14 днів) до закінчення строку чинності поточного сертифіката підписувача. У разі неотримання заяви про формування нового сертифіката підписувача у визначений термін ЦСК після закінчення строку чинності цього сертифіката скасовує його.

15. ФОРМУВАННЯ СЕРТИФІКАТІВ ВІДПОВІДАЛЬНИХ ОСІБ ЦСК

15.1. Генерація ключової пари

Відкритий та особистий ключі відповідальної особи ЦСК можуть бути згенеровані на основі стартових ключів, що отримані у адміністратора безпеки за допомогою:

- криптографічних засобів, що інтегровані до автоматизованого робочого місця відповідальної особи ЦСК;
- окремо виділеній робочій станції генерування ключів.

Під час генерування ключів автоматично створюється запит на формування сертифікату.

15.2. Формування запиту на формування сертифікату

Відповідальна особа ЦСК самостійно вносить запит на формування свого сертифіката до БД ПТК ЦСК.

15.3. Засвідчення запиту на формування сертифікату

Служба сертифікації ЦСК засвідчує запит на формування сертифікату відповідальної особи ЦСК.

15.4. Процедура формування сертифікату

Служба сертифікації ЦСК під час формування нового сертифіката створює запит на скасування поточного сертифіката, засвідчує його, формує та поширює СВС і тільки після цього формує новий сертифікат відповідальної особи ЦСК.

15.5. Терміни подачі заяви на формування сертифікату

Відповідальна особа не пізніше ніж за десять (14 днів) робочих днів до закінчення строку чинності поточного сертифіката генерує нові криптографічні ключі та ініціює процедуру формування нового сертифіката.

16. ФОРМУВАННЯ СЕРТИФІКАТУ ПОСЛУГИ ІНТЕРАКТИВНОГО ВИЗНАЧЕННЯ СТАТУСУ СЕРТИФІКАТУ

16.1. Генерація ключової пари

Служба сертифікації здійснює генерування відкритих та особистих ключів сервісу OCSP.

16.2. Формування запиту на формування сертифікату

Служба сертифікації вносить запит на формування сертифікату сервісу OCSP до БД ПТК ЦСК.

16.3. Засвідчення запиту на формування сертифікату

Служба сертифікації ЦСК засвідчує запит на формування сертифікату сервісу OCSP ЦСК.

16.4. Процедура формування сертифікату

Служба сертифікації ЦСК під час формування нового сертифікату сервісу OCSP створює запит на скасування поточного сертифіката сервісу OCSP, потім засвідчує його, формує та

поширює СВС і тільки після цього формує новий сертифікат OCSP.

16.5. Терміни подачі заяви на формування сертифікату

Служба сертифікації ЦСК не пізніше ніж за десять робочих днів до закінчення строку чинності поточного сертифіката генерує нові криптографічні ключі та здійснює процедуру формування нового сертифіката OCSP.

17. ФОРМУВАННЯ СЕРТИФІКАТУ ПОСЛУГИ ФІКСУВАННЯ ЧАСУ

17.1. Генерація ключової пари

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

17.2. Формування запиту на формування сертифікату

ЦСК подає до служби реєстрації ЗЦ НБУ заяву про формування сертифікату послуги фіксування часу та запит на формування сертифікату послуги фіксування часу.

17.3. Засвідчення запиту на формування сертифікату

Служба сертифікації ЗЦ НБУ засвідчує запит на формування сертифікату послуги фіксування часу ЦСК.

17.4. Терміни подачі заяви на формування сертифікату

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

18. ЗМІНА СТАТУСУ СЕРТИФІКАТІВ ПІДПИСУВАЧІВ

18.1. Чинність зміни статусу сертифікату

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

18.2. Зміна статусу блокованих сертифікатів

Підписувач зобов'язаний протягом не більше 30 календарних днів після блокування сертифіката скасувати або поновити його. Поновлення сертифіката підписувача можливе лише для сертифікатів, що заблоковані й термін дії яких не закінчився.

18.3 Скасування сертифікату без його попереднього блокування

Дозволяється на розсуд підписувача скасувати сертифікат без його блокування.

18.4. Умови блокування або поновлення сертифікату

ЦСК негайно блокує/поновлює сертифікат підписувача в разі:

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

18.5. Умови скасування сертифікату

ЦСК скасовує сертифікат підписувача в разі:

- подання заявником письмової заяви про скасування сертифіката підписувача до служби

реєстрації ЦСК;

- наявності рішення суду про скасування сертифіката 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 виданий фізичній особі, як представнику юридичної особи);
- надання заявником 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. Причини блокування або скасування сертифікату

Причинами, унаслідок яких заявник звертається до служби реєстрації ЦСК щодо блокування/скасування сертифіката підписувача, є:

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

18.7. Причини поновлення сертифікату

Причинами, унаслідок яких заявник звертається до служби реєстрації ЦСК щодо поновлення сертифіката 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.

18.8. Форми заяв про блокування або поновлення сертифікату

Заявник може подати до служби реєстрації ЦСК звернення щодо блокування/поновлення сертифіката підписувача у вигляді:

- письмової заяви, див. Додаток А;
- заяви в усній формі телефоном.

18.9. Заява про скасування сертифікату

Заявник подає до служби реєстрації ЦСК звернення щодо скасування сертифіката підписувача у вигляді письмової заяви.

18.10. Обов'язкова інформація в заявці в усній формі від підписувача

Заявник (підписувач) подає заяву в усній формі засобами телефонного зв'язку за номерами ЦСК. У заяві в усній формі повідомляються:

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

Блокування сертифіката підписувача за заявою в усній формі здійснюється тільки в разі позитивної автентифікації заявника (збіг ідентифікаційних даних підписувача, заявника, серійного

номера сертифіката підписувача та фрази-пароля, переданої в усній заяві, з інформацією з реєстру ЦСК).

18.11. Обов'язкове письмове підтвердження заяви, поданої в усній формі

Заява про блокування сертифіката підписувача в усній формі має бути підтверджена письмовою заявою протягом двох робочих днів з часу прийняття службою реєстрації ЦСК відповідного звернення.

18.12. Збереження документальних підстав для зміни статусу

Документи та записи телефонних дзвінків, що були підставою для зміни статусу сертифіката підписувача, фіксуються та зберігаються в ЦСК.

18.13. Приймання заявок на зміну статусу

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

18.14. Процедура зміни статусу сертифікату

ЦСК здійснює зміну статусу сертифіката підписувача в такому порядку.

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

- опрацьовує її згідно з вимогами цього Регламенту;
- створює запит на зміну статусу поточного сертифіката підписувача в разі виконання заявником усіх умов, визначених цим Регламентом.

2. Служба сертифікації ЦСК:

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

18.16. Терміни зміни статусу сертифікату

ЦСК здійснює зміну статусу сертифіката підписувача, зареєстрованого в ЦСК, становить не більше:

- для працівника банка до однієї години;
- для клієнту банка до однієї години.

18.17. Зміна ідентифікаційних даних

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 разом із заявою про зміну ідентифікаційних даних підписувача подає заяву про формування нового сертифіката підписувача в ЦСК, якщо дані, які змінюються, унесені до сертифіката підписувача. Разом із заявою необхідно подати документи, що підтверджують ці зміни.

19. ЗМІНА СТАТУСУ СЕРТИФІКАТІВ ВІДПОВІДАЛЬНИХ ОСІБ ЦСК

19.1. Чинність зміни статусу сертифікату

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

19.2. Строки зміни статусу сертифікатів

Строк блокування сертифікатів 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 самостійно або за зверненням відповідальної особи ЦСК. Поновлення сертифіката відповідальної особи ЦСК можливе лише для сертифікатів, що заблоковані й строк блокування яких не закінчився. Якщо до закінчення строку блокування сертифікат не був поновлений, то ЦСК скасовує цей сертифікат.

19.3. Скасування сертифікату без його попереднього блокування

Дозволяється на розсуд служби безпеки ЦСК скасувати сертифікат відповідальної особи ЦСК без його блокування.

19.4. Форми звернень про зміну статусу

Відповідальна особа ЦСК для зміни статусу свого сертифіката подає відповідну заяву до служби безпеки ЦСК (ЦСК самостійно визначає форму письмової заяви та її зміст відповідно до Додатку В).

19.5. Умови зміни статусу сертифікату

ПТК ЦСК негайно змінює статус сертифіката відповідальної особи ЦСК у разі подання службою безпеки ЦСК до служби реєстрації ЦСК відповідної заяви.

19.6. Причини звернення відповідальної особи до служби безпеки ЦСК для блокування або скасування сертифікату

Причинами, унаслідок яких відповідальна особа ЦСК звертається до служби безпеки ЦСК щодо блокування/скасування свого сертифіката, 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;
- інші причини, визначені цим Регламентом та законодавством України у сфері ЕЦП.

19.7. Причини звернення служби безпеки ЦСК до служби сертифікації ЦСК для блокування або скасування сертифікату

Причинами, унаслідок яких служба безпеки ЦСК звертається до служби сертифікації ЦСК щодо блокування/скасування сертифіката відповідальної особи ЦСК, є:

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

19.8. Причини звернення відповідальної особи до служби безпеки ЦСК для поновлення сертифікату

Причинами, унаслідок яких відповідальна особа ЦСК звертається до служби безпеки ЦСК щодо поновлення свого сертифіката, 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.

19.9. Причини звернення служби безпеки ЦСК до служби сертифікації ЦСК для поновлення сертифікату

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

19.10. Збереження документальних підстав для зміни статусу

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

19.11. Процедура зміни статусу

Служба реєстрації ЦСК під час подання службою безпеки ЦСК заяви про зміну статусу сертифіката відповідальної особи ЦСК:

- опрацьовує її згідно з вимогами цього Регламенту;
- створює запит на зміну статусу поточного сертифіката відповідальної особи ЦСК та засвідчує його;
- уносить відповідні зміни до реєстру чинних сертифікатів із зазначенням дати, часу та причин зміни статусу сертифіката відповідальної особи ЦСК.

19.12. Терміни зміни статусу сертифікату

Служба реєстрації ЦСК здійснює зміну статусу сертифіката відповідальної особи ЦСК протягом не більше однієї години з часу подання заяви службою безпеки ЦСК.

19.13. Зміна ідентифікаційних даних

Відповідальна особа ЦСК протягом одного робочого дня повідомляє службу безпеки ЦСК про зміну своїх ідентифікаційних даних, які внесено до реєстру, шляхом подання відповідної заяви. Відповідальна особа ЦСК разом із заявою про зміну своїх ідентифікаційних даних подає заяву про формування нового сертифіката, якщо дані, які змінюються, внесено до сертифіката відповідальної особи ЦСК. Разом із заявою необхідно подати документи, що підтверджують ці зміни.

20. ЗМІНА СТАТУСУ СЕРТИФІКАТІВ ПОСЛУГИ ІНТЕРАКТИВНОГО ВИЗНАЧЕННЯ СТАТУСУ СЕРТИФІКАТУ

20.1. Чинність зміни статусу сертифікату

Зміна статусу сертифіката OCSP набирає чинності з часу внесення відповідних змін у СВС та до реєстру чинних сертифікатів.

20.2. Терміни блокування сертифікатів

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

20.3. Скасування сертифікату без його попереднього блокування

Дозволяється на розсуд служби сертифікації ЦСК скасувати сертифікат OCSP без його блокування.

20.4. Умови блокування або скасування сертифікату

Служба сертифікації ЦСК негайно блокує/скасовує сертифікат OCSP у разі:

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

20.5. Причини поновлення сертифікату

Служба сертифікації ЦСК негайно поновлює сертифікат OCSP у разі виявлення недостовірності даних про:

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

20.6. Процедура зміни статусу сертифікату

Служба сертифікації ЦСК під час зміни статусу сертифіката OCSP:

- створює запит на зміну статусу поточного сертифіката OCSP та засвідчує його;
- уносить відповідні зміни до реєстру чинних сертифікатів із зазначенням дати, часу та причин зміни статусу сертифіката OCSP;
- формує СВС;
- поширює інформацію про зміну статусу сертифіката OCSP згідно з вимогами цього Регламенту.

20.7. Терміни зміни статусу сертифікату

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

20.8. Збереження документальних підстав для зміни статусу

Документи, що були підставою для зміни статусу сертифіката OCSP, зберігаються в ЦСК.

21. ЗМІНА СТАТУСУ СЕРТИФІКАТІВ ПОСЛУГИ ФІКСУВАННЯ ЧАСУ

21.1. Терміни зміни статусу сертифікату

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

21.2. Процедура зміни статусу сертифікату

Служба сертифікації ЦСК банку, для зміни статусу сертифіката 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. ІНФОРМАЦІЙНИЙ РЕСУРС ЦСК

22.1. Призначення

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, зразок договору про надання підписувачам послуг ЕЦП, форми заяв тощо);

- сертифікати ЦСК;
- СВС, що містить інформацію про статус сертифікатів ЦСК та підписувачів.

22.2. Публікація СВС та сертифікатів

Публікація СВС і сертифікатів ЦСК та підписувачів на інформаційному ресурсі ЦСК здійснюється відразу після їх формування та перевірки власником сертифіката/заявником даних, що вносяться до сертифіката.

22.3. Представлення інформації на інформаційному ресурсі

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

22.4. Протоколи доступу до СВС, сертифікатів підписувачів та ЦСК

Сертифікати ЦСК та СВС розміщуються:

- у складі web-сторінок на HTTP-сервері інформаційного ресурсу ЦСК;
- в інформаційному дереві LDAP-каталога на LDAP-сервері.

22.5. Терміни оновлення інформації у LDAP-каталозі

Публікація сертифікатів ЦСК та підписувачів в інформаційному дереві LDAP-каталога здійснюється автоматично з інтервалом п'ять хвилин. Публікація СВС в інформаційному дереві LDAP-каталога здійснюється автоматично з інтервалом синхронізації п'ять хвилин.

22.6. Доступ до СВС на HTTP-сервері

Доступ СВС та дельта-СВС до HTTP-сервера здійснюється за DNS-ім'ям www.ca.kredobank.com.ua за протоколом HTTP/HTTPS (номер TCP-порта 80/443).

23. ПОШИРЕННЯ ІНФОРМАЦІЇ ПРО СТАТУС СЕРТИФІКАТІВ

23.1. Шляхи поширення інформації про статус сертифікатів

ЦСК поширює інформацію про статус сертифіката:

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

23.2. Доступ до OCSP-серверу

Взаємодія з OCSP-сервером для отримання послуг визначення статусу сертифікатів забезпечується шляхом використання клієнтського ПЗ. Таке ПЗ повинно відповідати технічним специфікаціям та форматам даних, визначеним законодавством України.

23.3. Обов'язкова інформація, що міститься у СВС

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.

23.4. Шляхи поширення СВС

ЦСК поширює СВС шляхом їх розміщення на інформаційному ресурсі ЦСК.

23.5. Види СВС

ЦСК формує та публікує СВС двох типів:

- повний список;
- частковий список.

23.6. Терміни оновлення СВС

Повний список виходить один раз на добу містить інформацію про всі відкликані сертифікати, які були сформовані в ЦСК за допомогою чинного власного особистого ключа ЦСК. Частковий список формується та поширюється кожні 5 хвилин та містить інформацію про всі відкликані сертифікати, статус яких був змінений у межах часу випуску останнього повного СВС та часу формування поточного часткового СВС.

23.7. Використання сертифіката підписувача

Перед використанням сертифіката слід перевірити:

- термін дії сертифікату;
- статус сертифіката підписувача за поточним СВС або за допомогою OCSP-запиту;
- автентичність і цілісність СВС та/чи отриманої OCSP-відповіді.

23.8. Умова користування сертифікатом

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

24. ПОСЛУГА ФІКСУВАННЯ ЧАСУ

24.1. Фіксування часу

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

24.2. Доступ до TSP-сервер

Взаємодія з TSP-сервером для отримання послуг фіксування часу забезпечується шляхом використання клієнтського ПЗ. Таке ПЗ повинно відповідати технічним специфікаціям та форматам даних, визначених законодавством України.

25. СИНХРОНІЗАЦІЯ ЧАСУ В ПТК ЦСК

25.1. Точність

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).

25.2. Синхронізація із всесвітнім координованим часом

ПТК основного і резервного ЦСК, що розміщені у окремих ЦОД забезпечує синхронізацію із всесвітнім координованим часом (UTC) з точністю до однієї секунди за допомого 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 період.

25.3. Сервери часу для синхронізації

ЦСК синхронізує час із серверами часу Національного банку України.

25.4. Налаштування синхронізації

Системний адміністратор ЦСК налаштовує NTP з використанням засобів ОС.

26. ПОРЯДОК АРХІВНОГО ЗБЕРІГАННЯ ДОКУМЕНТОВАНОЇ ІНФОРМАЦІЇ

26.1. Перелік документів для архівного зберігання

ЦСК здійснює архівне зберігання таких документів:

- сертифікати ЦСК, відповідальних осіб ЦСК та підписувачів (чинні, скасовані, блоковані);
- реєстр відповідальних осіб ЦСК та підписувачів;
- копії і оригінали документів на папері або документи в електронному вигляді, що подані заявниками (підписувачами, які є працівниками банку) під час реєстрації, формування, зміни статусу сертифіката, зміни даних підписувачів;
- СВС;
- журнали аудиту та документи ЦСК, у тому числі протоколи роботи ПТК ЦСК.

26.2. Вимоги до зберігання документів

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.

26.3. Документи постійного зберігання

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

26.4. Документи тимчасового зберігання

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

26.5. Виділення та знищення архівних документів

Видалення 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.

26.7. Умови надання архівної інформації

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.

27. ПОРЯДОК УНЕСЕННЯ ЗМІН ДО РЕГЛАМЕНТУ

27.1. Внесення змін і їх оприлюднення

Зміни до цього Регламенту вносяться відповідно до законодавства України.

У разі внесення змін до цього Регламенту відповідальні особи ЦСК та підписувачі інформуються про це шляхом:

- розміщення оновленого Регламенту та оголошення про відповідні зміни на інформаційному ресурсі ЦСК;
- розсилання зазначених змін електронною поштою.

27.2. Підстави для внесення змін

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. Якщо ці зміни будуть суперечити умовам договорів та інших правочинів, що мають відношення до ЦСК, необхідно протягом 30 днів з дня набрання чинності таких змін, внести відповідні зміни до цих договорів та інших правочинів.

ЦСК має право в односторонньому порядку вносити зміни і доповнення до Регламенту. Повідомлення про внесення змін та доповнень до Регламенту, а також уточнена редакція Регламенту розміщується на електронному інформаційному ресурсі ЦСК в мережі Інтернет не пізніше ніж за 10 (десять) робочих днів до вступу змін та доповнень у дію.

Усі зміни та доповнення, що відносяться до Регламенту у зв'язку із змінами законодавства, вступають у силу одночасно із змінами та доповненнями до відповідних нормативних актів.

Усі зміни та доповнення до Регламенту, з моменту їх вступу у дію, однаково поширюються на всіх підписувачів ЦСК, що приєдналися до Регламенту, в тому числі і на тих, що приєдналися до Регламенту раніше за дату вступу у дію змін та доповнень.

27.3. Згода користувачів ЦСК з умовами

Якщо підписувач ЦСК не згоден із внесеними змінами та доповненнями, він має право припинити користування послугами ЕЦП від ЦСК.