Товариство з обмеженою відповідальністю
«Центр сертифікації ключів «Україна»

ПОГОДЖЕНО

Перший заступник Голови Державної служби спеціального зв'язку та захисту інформації України

_____ О.Г.Цуркан

“___”_____ 2012 р.

ЗАТВЕРДЖУЮ

Директор ТОВ «Центр сертифікації ключів «Україна»

_____ О.Л. Меньшиков

“___”_____ 2012 р.

Регламент
роботи акредитованого центру сертифікації ключів товариства з обмеженою відповідальністю «Центр сертифікації ключів «Україна»

На 36 аркушах

Київ 2012

Зміст

Перелік умовних позначень та скорочень 4
1. Загальні положення....6
1.1. Терміни та визначення....6
1.2. Ідентифікаційні дані АЦСК 6
1.3. Порядок внесення змін до Регламенту 7
2. Перелік суб'єктів, задіяних в обслуговуванні і використанні сертифікатів 7
2.1. АЦСК....7
2.2. ВПР....8
2.3. Підписувачі та користувачі....8
3. Використання сертифікатів....9
3.1. Сфери використання сертифікатів 9
3.2. Обмеження щодо використання сертифікатів 9
3.3. Термін дії сертифікатів....10
4. Порядок розповсюдження відкритої інформації АЦСК 10
4.1. Перелік інформації, яка розміщена на електронному інформаційному ресурсі АЦСК 10
4.2. Порядок публікації сертифікатів АЦСК та сертифікатів серверів АЦСК 11
4.3. Порядок публікації сертифікатів підписувачів....11
4.4. Порядок публікації списку відкликаних сертифікатів....11
5. Ідентифікація та автентифікація....11
5.1. Механізм підтвердження володіння заявником (підписувачем) відповідним особистим ключем 11
5.2. Порядок проведення процедури реєстрації заявників 12
5.2.1. Встановлення заявника....12
5.2.2. Встановлення особи та повноважень представника заявника....13
5.2.3. Документи, необхідні для реєстрації заявника 13
5.2.4. Розгляд документів, що надаються для реєстрації заявника 14
5.3. Захист персональних даних підписувачів 15
5.4. Порядок повторної реєстрації заявника після закінчення терміну дії сертифіката 15
5.5. Автентифікація заявника (підписувача) під час звернення щодо заміни сертифіката 16
5.6. Автентифікація підписувача під час звернення до АЦСК щодо зміни статусу сертифіката16
6. Процедури та механізми обслуговування сертифікатів....16
6.1. Порядок подання заявки на сертифікацію....16
6.2. Порядок формування сертифіката....17
6.3. Повторне формування сертифіката....17
6.4. Використання сертифіката та особистого ключа підписувача....18
6.4.1. Обов'язки підписувача 18
6.4.2. Права підписувача....19
6.4.3. Обов'язки користувача....19
6.5. Скасування сертифікатів 19
6.5.1. Підстави для скасування сертифікатів....20
6.5.2. Обставини, за яких сертифікат ключа повинен бути скасований підписувачем.....20
6.5.3. Порядок скасування сертифікатів 20
6.5.3.1. Скасування сертифіката за заявою у письмовій формі 21
6.5.3.2. Скасування сертифіката за заявою в електронній формі 21
6.6. Блокування сертифікатів....21
6.6.1. Підстави для блокування сертифікатів....21
6.6.2. Порядок блокування сертифікатів....21
6.6.2.1. Блокування сертифіката за заявою в усній формі....22
6.6.2.2. Блокування сертифіката за заявою в електронній формі....22
6.6.2.3. Блокування сертифіката за заявою у письмовій формі....22

6.7. Поновлення сертифікатів 22
6.7.1. Підстави для поновлення сертифікатів 23
6.7.2. Порядок поновлення сертифікатів 23
6.8. Розповсюдження інформації про статус сертифікатів 23
6.9. Закінчення строку чинності сертифіката підписувача 23
6.10. Порядок надання послуги фіксування часу 24
7. Управління та операційний контроль 24
7.1. Фізичне середовище 24
7.1.1. Приміщення АЦСК 24
7.1.2. Пропускний і внутрішній режим 25
7.2. Процедурний контроль 25
7.2.1. Права, обов'язки та відповідальність АЦСК 25
7.2.1.1. Права АЦСК 25
7.2.1.2. Обов'язки АЦСК 26
7.2.1.3. Відповідальність АЦСК 26
7.2.2. Склад організаційної структури АЦСК 27
7.2.2.1. Адміністрація 27
7.2.2.2. Відділ сертифікації 28
7.2.2.3. Відділ реєстрації 28
7.2.2.4. Архівний відділ 28
7.2.2.5. Служба захисту інформації 29
7.2.2.6. ВПР 30
7.3. Порядок ведення журналів аудиту АС АЦСК 30
7.4. Порядок ведення архівів та зберігання документованої інформації 31
8. Управління ключами та забезпечення захисту особистого ключа АЦСК 32
8.1. Порядок генерації ключів підписувачів 32
8.1.1. Генерація ключів на робочій станції підписувача 32
8.1.2. Генерація ключів на робочій станції АЦСК 33
8.2. Порядок генерації та захисту особистих ключів АЦСК 33
8.3. Порядок резервування та відновлення особистих ключів АЦСК 34
8.4. Протоколювання операцій з особистим ключем АЦСК 34
8.5. Строки дії особистих ключів АЦСК та порядок їх заміни 35
8.5.1. Порядок планової зміни ключів АЦСК та посадових осіб АЦСК 35
8.5.2. Порядок позапланової зміни ключів АЦСК 36

Перелік умовних позначень та скорочень

У даному Регламенті умовні позначення та скорочення, наявні в ньому, використовуються у такому значенні:

Умовні позначення та скорочення	Опис
АС	Автоматизована система
АЦСК	Акредитований центр сертифікації ключів ТОВ «Центр сертифікації ключів «Україна»
БД	База даних
ВПР	Відокремлений пункт реєстрації
Договір	Договір про надання послуг електронного цифрового підпису
ДСТСЗІ СБ України	Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України
ЕЦП	Електронний цифровий підпис
Заявка	Електронна заявка (запит) на сертифікацію відкритого ключа
Картка приєднання	Картка приєднання до Договору про надання послуг електронного цифрового підпису
КЗІ	Криптографічний захист інформації
КСЗІ	Комплексна система захисту інформації
OCSP	Online Certificate Status Protocol
ПТК	Програмно-технічний комплекс
Правила	Наказ ДСТСЗІ СБ України «Про затвердження Правил посиленої сертифікації» № 3 від 13.01.2005 р. (із змінами, внесеними згідно з наказом ДСТСЗІ СБ України № 50 від 10.05.2006 р.)
Регламент	Регламент роботи акредитованого центру сертифікації ключів ТОВ «Центр сертифікації ключів «Україна»
Сайт АЦСК	Загальнодоступний електронний інформаційний ресурс АЦСК в мережі Інтернет за адресою http://uakey.com.ua
Сертифікат	Посилений сертифікат відкритого ключа
СКБД	Система керування базою даних
TSP	Time Stamp Protocol

ФОП	Фізична особа - підприємець
ЦЗО	Центральний засвідчувальний орган
ЦСК	Центр сертифікації ключів

1. Загальні положення

Регламент роботи акредитованого центру сертифікації ключів товариства з обмеженою відповідальністю «Центр сертифікації ключів «Україна» розроблений відповідно до чинного законодавства України, яке регулює питання у сфері ЕЦП, а саме:

- Закону України «Про електронний цифровий підпис» № 852-IV від 22.05.2003 р.;
- Закону України «Про електронні документи та електронний документообіг» № 851-IV від 22.05. 2003 р.;
- Постанови Кабінету Міністрів України «Про затвердження Порядку акредитації ЦСК сертифікації ключів» № 903 від 13.07.2004 р.;
- Наказу ДСТСЗІ СБ України «Про затвердження Правил посиленої сертифікації» № 3 від 13.01.2005 р. (із змінами, внесеними згідно з Наказом ДСТСЗІ СБ України № 50 від 10.05.2006 р.).

Цей Регламент встановлює загальний порядок діяльності АЦСК під час надання послуг ЕЦП, правила взаємодії АЦСК, підписувачів та користувачів, а також права, обов'язки та відповідальність обслуговуючого персоналу АЦСК та клієнтів.

Норми даного Регламенту є обов'язковими для виконання АЦСК, ВПР та для заявника (підписувача) з моменту подачі заявником (підписувачем) чи його уповноваженим представником комплекту необхідних документів до АЦСК і протягом строку дії договору, якщо інше не передбачене Регламентом.

З Регламентом можна ознайомитись безпосередньо в офісі АЦСК чи ВПР та на сайті АЦСК.

1.1. Терміни та визначення

У цьому Регламенті терміни вживаються у такому значенні:

- заявник — фізична або юридична особа, яка звертається до АЦСК з метою отримання послуг ЕЦП на підставі відповідного договору, укладеного між заявником та АЦСК;
- підписувач — особа, яка на законних підставах володіє особистим ключем, має відповідні йому відкритий ключ та сформований АЦСК сертифікат та від свого імені або за дорученням особи, яку вона представляє, накладає ЕЦП під час створення електронного документа;
- користувач — особа, яка використовує надійні засоби ЕЦП, сертифікати та дані про статус сертифікатів для перевірки ЕЦП.

Інші терміни та визначення, що вживаються в цьому Регламенті, визначені нормативно-правовими актами, що наведені в п. 1.

1.2. Ідентифікаційні дані АЦСК

Повне найменування	Товариство з обмеженою відповідальністю «Центр сертифікації ключів «Україна»
Скорочене найменування	ТОВ «Центр сертифікації ключів «Україна»
ЄДРПОУ	36865753
Місцезнаходження організації	04080, м. Київ, вул. Фрунзе, 102
Номери телефону/факсу	(044) 206-72-31/206-72-32

Адреса електронного інформаційного ресурсу АЦСК в мережі Інтернет	http://uakey.com.ua
Адреса електронної пошти	info@uakey.com.ua

1.3. Порядок внесення змін до Регламенту

АЦСК має право в односторонньому порядку вносити зміни та доповнення до Регламенту. Зміни та доповнення до Регламенту погоджуються з контролюючим органом у встановленому порядку.

Зміни та доповнення до Регламенту, що не пов'язані зі зміною чинного законодавства України, набувають чинності через 10 (десять) календарних днів з моменту їх розміщення на сайті АЦСК.

Всі зміни та доповнення, що вносяться до Регламенту у зв’язку із змінами законодавства, набувають чинності одночасно зі вступом у силу відповідних нормативно-правових актів.

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

Якщо підписувач АЦСК не погоджується із внесеними змінами та доповненнями, він має право припинити використання свого сертифіката.

2. Перелік суб’єктів, задіяних в обслуговуванні і використанні сертифікатів

До суб’єктів, що задіяні в обслуговуванні і використанні сертифікатів належать:

- АЦСК;
- ВПР;
- підписувачі;
- користувачі.

2.1. АЦСК

АЦСК здійснює свою діяльність у сфері електронного документообігу, надання послуг ЕЦП підприємствам, установам та організаціям всіх форм власності, іншим суб’єктами господарської діяльності та фізичним особам на договірних засадах.

Перелік послуг ЕЦП, які може надавати АЦСК:

1) реєстрація підписувачів;
2) надання у користування засобів КЗІ, у тому числі надійних засобів ЕЦП;
3) допомога під час генерації відкритих та особистих ключів;
4) обслуговування сертифікатів підписувачів, що включає:
   - сертифікацію відкритих ключів підписувачів;
   - розповсюдження та зберігання сертифікатів;
   - управління статусом сертифікатів та розповсюдження інформації про їх статус.
5) надання послуг фіксування часу (позначки часу);
6) консультації щодо застосування ЕЦП за зверненнями підписувачів та користувачів АЦСК.

Надання зазначених послуг здійснюється АЦСК у відповідності до чинного законодавства України, цього Регламенту та на підставі укладеного Договору або Договору приєднання, укладеного шляхом підписання Картки приєднання.

2.2. ВПР

Для надання послуг ЕЦП на певній території АЦСК може створювати ВПР та (або) відряджати адміністраторів реєстрації до певного регіону.

ВПР є структурними (територіальними) підрозділами АЦСК, які здійснюють реєстрацію заявників та їх подальше обслуговування на відповідній території.

ВПР діють на підставі Положення про відокремлений пункт реєстрації та цього Регламенту.

Безпосереднє управління ВПР здійснюється АЦСК.

ВПР виконує такі функції:

- встановлює осіб, які звернулися до АЦСК з метою формування, скасування, блокування або поновлення сертифікатів;
- отримує і перевіряє дані, обов'язкові для формування сертифіката, а також дані, які вносяться у сертифікат на вимогу клієнта;
- проводить процедуру реєстрації заявників (підписувачів);
- отримує від користувачів та перевіряє заявки на формування, скасування, блокування та поновлення сертифікатів;
- надає консультації підписувачам під час генерації ключів, у разі отримання від них відповідного звернення, та вживає заходи щодо забезпечення захисту ключової інформації під час генерації;
- надає підписувачам консультації щодо умов та порядку надання і використання послуг ЕЦП;
- передає до АЦСК відомості та документи, що надаються заявниками (підписувачами) для формування або зміни статусу сертифіката.

Адміністратори реєстрації, яких відряджають до певних регіонів, надають послуги ЕЦП заявникам (підписувачам) у межах своїх функцій та повноважень згідно посадової інструкції.

Перелік ВПР АЦСК та відомості про місця їх розташування, а також перелік адміністраторів реєстрації, які працюють поза межами АЦСК (за наявності) та їх контактні дані публікуються на сайті АЦСК.

2.3. Підписувачі та користувачі

Використання сертифікатів, сформованих АЦСК здійснюється підписувачами, а також користувачами.

Підписувачі мають договірні відносини з АЦСК, на законних підставах володіють особистими ключами, мають відповідні відкриті ключі та сформовані АЦСК сертифікати. Підписувачі користуються послугами АЦСК в рамках договірних відносин з АЦСК.

У договорі повинно бути зазначено:

- обов'язки сторін, у тому числі щодо обов'язковості використання надійних засобів ЕЦП;
- умови надання доступу користувачам до сертифіката підписувача (умови публікації сертифіката);
- інформацію про обмеження використання сертифіката.

Користувачі не мають договірних відносин з АЦСК, однак при цьому можуть використовувати загальнодоступну інформацію з сайту АЦСК, а також користуватися послугами АЦСК, що не потребують автентифікації. Користувачі можуть використовувати надійні засоби ЕЦП для перевірки ЕЦП підписувачів АЦСК.

3. Використання сертифікатів

В АЦСК можуть формуватись та (або) використовуватись наступні типи сертифікатів:

- сертифікат АЦСК;
- сертифікат посадової особи АЦСК;
- сертифікат сервера АЦСК;
- сертифікат підписувача АЦСК;
- сертифікат шифрування даних.

3.1. Сфери використання сертифікатів

Сертифікати можуть використовуватись в таких сферах:

Тип сертифіката	Сфера використання сертифіката
Сертифікат АЦСК	Використовується для перевірки ЕЦП, накладеного на сертифікати та списки відкликаних сертифікатів, сформовані АЦСК.
Сертифікат посадової особи АЦСК	Використовується для ідентифікації та автентифікації посадової особи в ПТК АЦСК та (або) для перевірки ЕЦП посадової особи.
Сертифікат сервера АЦСК	Використовується для організації надання послуг, що потребують накладення ЕЦП на відповіді, які формує сервер АЦСК (наприклад, позначки часу, що надаються за протоколом TSP, інформація про статус сертифіката, яка розповсюджується за протоколом OCSP, та інші послуги).
Сертифікат підписувача АЦСК	Сертифікат підписувача використовується для перевірки ЕЦП, що був накладений власником відповідного сертифіката, відповідно до діючого законодавства у сфері ЕЦП. Сертифікат може використовуватись для ідентифікації користувачів інформаційно-телекомунікаційних систем, в яких застосовуються механізми автентифікації з використанням ЕЦП.
Сертифікат шифрування	Використовується для підтвердження відповідності відкритого ключа його власнику під час криптографічного захисту інформації шляхом направленого шифрування даних.

3.2. Обмеження щодо використання сертифікатів

Сертифікати АЦСК і відповідні до них особисті ключі АЦСК можуть використовуватись виключно для формування сертифікатів та списків відкликаних сертифікатів.

Сертифікати серверів АЦСК і відповідні до них особисті ключі можуть використовуватись лише для надання відповідних послуг. Призначення сертифіката сервера АЦСК зазначається у розширеному полі сертифіката "Уточнене призначення відкритого ключа".

Сертифікати посадових осіб АЦСК і відповідні до них особисті ключі можуть використовуватись посадовими особами АЦСК лише під час виконання своїх посадових обов'язків. Ознака того, що сертифікат використовується як сертифікат посадової особи АЦСК, зазначається у розширеному полі сертифіката "Уточнене призначення відкритого ключа".

Для сертифікатів підписувачів встановлюється обмеження максимальної вартості фінансової трансакції, для якої сертифікат може бути використаний. Це обмеження обумовлюється у договорі надання послуг та вноситься до сертифіката підписувача у відповідне поле.

Сертифікати шифрування використовуються виключно для підтвердження відповідності відкритого ключа його власнику під час направленого шифрування даних. Ознака того, що сертифікат використовується для шифрування, зазначається у розширеному полі сертифіката "Сфера використання відкритого ключа".

АЦСК має право встановлювати інші обмеження сфери використання сформованих ним сертифікатів. Інформація щодо обмеження сфери використання сертифіката зазначається у розширеному полі сертифіката "Уточнене призначення відкритого ключа".

3.3. Термін дії сертифікатів

Термін дії сертифікатів АЦСК не може перевищувати п'ять років.

Термін дії всіх інших сертифікатів, сформованих АЦСК, не може перевищувати двох років.

4. Порядок розповсюдження відкритої інформації АЦСК

Доступ до відкритої інформації здійснюється через електронний інформаційний загальнодоступний ресурс АЦСК в мережі Інтернет (сайт АЦСК), який має адресу http://uakey.com.ua. Доступ до інформації здійснюється за протоколом HTTP.

Інформація, що публікується на електронному інформаційному ресурсі АЦСК, є загальнодоступною. АЦСК застосовує організаційні заходи та використовує технічні засоби захисту від несанкціонованої модифікації цієї інформації.

4.1. Перелік інформації, яка розміщена на електронному інформаційному ресурсі АЦСК

На сайті АЦСК розміщена наступна інформація:

- сертифікати АЦСК;
- сертифікати серверів АЦСК;
- сертифікати підписувачів, сформовані АЦСК (у разі згоди їх власників на публікацію);
- чинні списки відкликаних сертифікатів;
- чинний Регламент;
- типовий договір;
- режим роботи АЦСК;

- адреса АЦСК та перелік ВПР з адресами (за наявності);
- перелік послуг ЕЦП, що надаються АЦСК, та порядок їх надання;
- перелік документів, необхідних для реєстрації заявника, та документів, за якими проходить автентифікація та ідентифікація заявника;
- вартість послуг ЕЦП.

На сайті АЦСК може додатково розміщуватись будь-яка інша інформація.

4.2. Порядок публікації сертифікатів АЦСК та сертифікатів серверів АЦСК

Після формування сертифікати АЦСК та сертифікати серверів АЦСК (сервера позначок часу, сервера визначення статусу сертифіката тощо) публікуються на сайті АЦСК.

4.3. Порядок публікації сертифікатів підписувачів

Сертифікати підписувачів на сайті АЦСК публікуються за згодою їх власників. Інформація про згоду або незгоду підписувача або заявника на публікацію сертифікатів на сайті АЦСК зазначається в договорі.

Сертифікат, що формується АЦСК, публікується на сайті АЦСК (за наявності згоди його власника) не пізніше, ніж через дві години після формування.

В подальшому підписувач або заявник можуть змінити статус публікації сертифіката шляхом подання до АЦСК письмової заяви встановленого зразка.

4.4. Порядок публікації списку відкликаних сертифікатів

Список відкликаних сертифікатів публікується на сайті АЦСК одразу після його формування.

АЦСК формує списки відкликаних сертифікатів двох видів:

- повний список відкликаних сертифікатів;
- частковий список відкликаних сертифікатів.

Повний список відкликаних сертифікатів публікується один раз на сім днів та містить інформацію про відкликані сертифікати за весь період роботи АЦСК.

Частковий список публікується кожні дві години та містить інформацію про всі відкликані сертифікати, статус яких був змінений в інтервалі між часом формування останнього повного списку та часом формування поточного часткового списку.

У випадку одночасного використання декількох діючих особистих ключів АЦСК і відповідних до них сертифікатів, АЦСК може вести декілька списків відкликаних сертифікатів, підписаних різними особистими ключами АЦСК. В такому разі всі вони публікуються на сайті АЦСК у наведеному вище порядку.

5. Ідентифікація та автентифікація

5.1. Механізм підтвердження володіння заявником (підписувачем) відповідним особистим ключем

Відкритий ключ заявника (підписувача) подається на сертифікацію виключно у вигляді самопідписаного запиту формату PKCS#10 - заявки, яка засвідчується ЕЦП за допомогою особистого ключа, що йому відповідає.

У разі, якщо особистий та відкритий ключі були згенеровані поза межами АЦСК, під час реєстрації засобами ПТК АЦСК здійснюється перевірка щодо володіння підписувачем особистим ключем, який відповідає відкритому ключу, наданому для формування сертифіката. Підтвердження володіння заявником (підписувачем) відповідним особистим ключем здійснюється без розкриття його особистого ключа шляхом перевірки ЕЦП заявки за допомогою відкритого ключа, що міститься у заявці.

5.2. Порядок проведення процедури реєстрації заявників

До початку формування сертифікатів для юридичних осіб, фізичних осіб - підприємців або фізичних осіб АЦСК здійснює встановлення особи заявника (фізичної або юридичної особи). Встановлення особи заявника здійснюється адміністратором реєстрації АЦСК за особистої присутності заявника або присутності його уповноваженого представника в АЦСК або ВПР, або за місцем знаходження заявника адміністратором реєстрації АЦСК.

Крім цього, під час реєстрації, відповідно до цього Регламенту, встановлюється особа представника заявника та його повноваження.

Перед укладенням договору заявник (уповноважений представник) повинен ознайомитись з умовами обслуговування сертифікатів, що передбачені політикою сертифікації та цим Регламентом, зокрема:

- зобов'язаннями та відповідальністю АЦСК стосовно обслуговування сертифікатів ключів;
- зобов'язаннями та відповідальністю заявника (підписувача) при використанні сертифіката та зберіганні особистого ключа;
- умовами та порядком використання підписувачем свого сертифіката відкритого ключа;
- терміном зберігання даних про заявників (підписувачів), які отримує АЦСК при реєстрації;
- відомостями про надійні засоби ЕЦП, що можуть використовуватися для генерації ключів, формування та перевірки ЕЦП.

Заявник (уповноважений представник) для проходження процедури реєстрації подає до АЦСК чи ВПР комплект необхідний документів. Адміністратор реєстрації переглядає документи і приймає рішення про проведення реєстрації заявника чи про відмову в ній.

5.2.1. Встановлення заявника

Встановлення заявника – юридичної особи здійснюється за установчими документами юридичної особи (статутом, положенням) або копіями таких документів, які нотаріально засвідчені відповідно до законодавства України.

Встановлення фізичної особи - підприємця здійснюється на підставі свідоцтва про державну реєстрацію або виписки чи витягу з Єдиного державного реєстру юридичних осіб та фізичних осіб-підприємців, або копії одного з цих документів, засвідченої у встановленому порядку, та паспорта або іншого документа, який посвідчує особу, відповідно до законодавства України.

Встановлення заявника - фізичної особи здійснюється за її паспортом або іншим документом, який посвідчує особу, відповідно до законодавства України.

5.2.2. Встановлення особи та повноважень представника заявника

Якщо неможлива особиста присутність заявника (підписувача) під час реєстрації, його може представляти довірена особа – представник. У цьому випадку заявник видає представнику доручення (довіреність) відповідного зразка.

Встановлення особи представника здійснюється за його паспортом або іншим документом, який посвідчує особу, відповідно до законодавства України. Повноваження представника встановлюються за довіреністю (дорученням).

Представник може бути уповноважений на вчинення лише тих правочинів, право на вчинення яких має особа, яку він представляє.

Довіреність (доручення) представника засвідчується:

- для юридичних осіб – підписом уповноваженої особи (керівника) та відбитком печатки юридичної особи;
- для ФОП:
  - якщо у ФОП є печатка - підписом ФОП та відбитком його печатки;
  - якщо у ФОП відсутня печатка – нотаріально.
- для фізичних осіб – нотаріально.

5.2.3. Документи, необхідні для реєстрації заявника

Для реєстрації заявника – юридичної особи уповноважена особа надає такі документи:

- заповнений та підписаний договір - у двох примірниках або заповнену та підписану заявником картку приєднання до електронного договору - в одному примірнику;
- оригінал установчого документа юридичної особи (статуту, положення) або його нотаріально засвідчену копію (для ознайомлення);
- оригінал свідоцтва про державну реєстрацію або виписки чи витягу з Єдиного державного реєстру юридичних осіб та фізичних осіб-підприємців, або копію одного з цих документів, засвідчену нотаріально або державним реєстратором, або підписом керівника та печаткою юридичної особи;
- копії паспортів підписувачів – представників заявника або інших документів, що посвідчують особу, відповідно до законодавства України, засвідчені відповідними підписувачами;
- копії довідок про присвоєння ідентифікаційних номерів (карток фізичних осіб – платників податку) підписувачів – представників заявника, засвідчені відповідними підписувачами;
- копії документів про призначення на посаду підписувачів – представників заявника, засвідчені заявником;
- заявки на формування сертифікатів, засвідчені відповідними підписувачами (встановлена форма заявки на формування сертифіката розміщена на інформаційному ресурсі АЦСК).

Для реєстрації заявника – відокремленого підрозділу (філії, представництва) юридичної особи уповноважена особа надає такі документи:

- заповнений та підписаний Договір - у двох примірниках або заповнену та підписану заявником Картку приєднання до електронного Договору - в одному примірнику;

- оригінал установчого документа відокремленого підрозділу (філії, представництва) юридичної особи (положення) або його нотаріально засвідчену копію (для ознайомлення);
- оригінал довідки із управління статистики про внесення відомостей про відокремлений підрозділ до ЄДРПОУ або її копію, засвідчену нотаріально, або підписом керівника та печаткою відокремленого підрозділу (філії, представництва) юридичної особи;
- копії паспортів підписувачів – представників заявника або інших документів, що посвідчують особу, відповідно до законодавства України, засвідчені відповідними підписувачами;
- копії довідок про присвоєння ідентифікаційних номерів підписувачів – представників заявника, засвідчені відповідними підписувачами;
- копії документів про призначення на посади підписувачів – представників заявника, засвідчені заявником;
- заявки на формування сертифікатів, засвідчені відповідними підписувачами.

Для реєстрації заявника - ФОП надаються такі документи:

- заповнений та підписаний договір - у двох примірниках або заповнену та підписану картку приєднання до електронного договору - в одному примірнику;
- оригінал свідоцтва про державну реєстрацію або виписки чи витягу з Єдиного державного реєстру юридичних осіб та фізичних осіб-підприємців, або копію одного з цих документів, засвідчену нотаріально або державним реєстратором; за наявності печатки у ФОП - копія може бути засвідчена підписом та печаткою ФОП;
- паспорт або інший документ, який посвідчує особу, відповідно до законодавства України, та його копія, засвідчена підписувачем;
- копія довідки про присвоєння ідентифікаційного номера (картки фізичної особи – платника податку) ФОП, засвідчена підписувачем;
- заявки на формування сертифікатів, засвідчені підписувачем.

Для реєстрації заявника - фізичної особи надаються такі документи:

- заповнений та підписаний договір - у двох примірниках або заповнену та підписану картку приєднання до електронного договору - в одному примірнику;
- копія паспорта фізичної особи - заявника або іншого документа, який посвідчує її особу, відповідно до законодавства України, засвідчена підписувачем;
- копію довідки про присвоєння ідентифікаційного номера (картки фізичної особи – платника податку) фізичної особи - заявника, засвідчену підписувачем;
- заявку на формування сертифіката, засвідчену підписувачем.

Якщо заявником подано оригінал документа або його нотаріально засвідчену копію, копія такого документа може бути засвідчена підписом посадової особи АЦСК та печаткою АЦСК.

Бланки договорів та деяких реєстраційних документів встановленої форми (доручення тощо) розміщуються на сайті АЦСК.

5.2.4. Розгляд документів, що надаються для реєстрації заявника

Адміністратор реєстрації встановлює особу заявника (уповноваженого представника), що проходить процедуру реєстрації.

Надані заявником (уповноваженим представником) документи розглядаються в його присутності.

Не приймаються до розгляду документи, які мають підчистки, помарки, дописки, закреслені слова, інші виправлення чи написи олівцем, а також пошкоджені, внаслідок чого їх текст неможливо прочитати.

За результатами розгляду наданих документів адміністратор реєстрації приймає рішення про відмову у реєстрації заявника в таких випадках:

- при відсутності всіх необхідних для реєстрації документів;
- при поданні неналежно засвідчених копій документів;
- при встановленні невідповідності фактичних даних тим, які зазначені у поданих на реєстрацію документах;
- при поданні неправильно сформованих заявок.

У разі відмови від реєстрації адміністратор реєстрації повертає надані документи заявнику (уповноваженому представнику) та роз'яснює причини відмови.

У разі прийняття позитивного рішення про реєстрацію, адміністратор реєстрації приймає документи, виконує встановлену процедуру взяття на облік отриманих документів, та передає заявку в АЦСК для формування сертифіката.

Із документів, що були надані заявником (уповноваженим представником) під час реєстрації, формується справа підписувача. Справа підписувача береться на облік шляхом реєстрації в журналі, який ведеться в електронному вигляді засобами програмно-технічного комплексу АЦСК.

Реєстрація заявника є підставою для генерації ключів заявника (у випадку генерації ключів у АЦСК або ВПР) та формування сертифіката підписувача.

5.3. Захист персональних даних підписувачів

Захист персональних даних підписувачів забезпечується шляхом застосування:

- організаційних заходів з обліку та зберігання справ підписувачів, зокрема:
  - формування справ підписувачів та їх облік;
  - призначення відповідальної особи за зберігання справ підписувачів та захист персональних даних;
  - обмеження доступу обслуговуючого персоналу до приміщення, де зберігаються справи підписувачів;
- організаційно-технічних та технічних заходів, реалізованих КСЗІ АС АЦСК, у тому числі:
  - використанням надійних засобів ЕЦП;
  - веденням журналів роботи системи;
  - застосуванням антивірусних засобів, міжмережевих екранів тощо.

У разі відрядження адміністратора реєстрації до певного регіону для надання послуг ЕЦП, він повинен забезпечити захист персональних даних підписувачів відповідно до законодавства України.

5.4. Порядок повторної реєстрації заявника після закінчення терміну дії сертифіката

Процедура повторної реєстрації заявника після закінчення терміну дії сертифіката ідентична процедурі первинної реєстрації заявника за єдиним винятком: при повторній реєстрації може здійснюватися не формування нової справи підписувача, а актуалізація документів у існуючій справі підписувача на підставі наданої заявником інформації.

5.5. Автентифікація заявника (підписувача) під час звернення щодо заміни сертифіката

У разі звернення заявника (підписувача) щодо заміни сертифіката внаслідок зміни реєстраційних даних або виникнення необхідності позапланової зміни ключів в АЦСК подається заявка на сертифікат, а також документи, що підтверджують достовірність зміни даних (за необхідності). Перед виконанням процедури заміни сертифіката адміністратор реєстрації здійснює ідентифікацію (встановлення) особи заявника та перевірку наданих відомостей.

5.6. Автентифікація підписувача під час звернення до АЦСК щодо зміни статусу сертифіката

В залежності від порядку звернення в АЦСК щодо блокування, скасування чи поновлення сертифіката, передбачені різні форми автентифікації підписувача та перевірки законності такого звернення:

- у разі письмового звернення заявника або підписувача щодо блокування, скасування чи поновлення сертифіката, чинність звернення встановлюється відповідно за власноручним підписом заявника та печаткою заявника (якщо заявник має печатку) або за власноручним підписом підписувача;
- у разі звернення шляхом направлення запиту в електронному вигляді на блокування або скасування сертифіката, чинність звернення встановлюється шляхом перевірки ЕЦП на запиті за допомогою чинного сертифіката підписувача;
- у разі звернення по телефону щодо блокування сертифіката чинність звернення встановлюється за парольною фразою, яка вказується підписувачем під час формування заявки.

6. Процедури та механізми обслуговування сертифікатів

6.1. Порядок подання заявки на сертифікацію

Для формування сертифіката використовується запит на формування сертифіката ключа – електронна заявка, яка створюється в процесі генерації особистого та відкритого ключів ЕЦП. Заявку може подавати заявник (уповноважений представник), що пройшов процедуру реєстрації, або підписувач (у разі позапланової заміни ключа).

Після здійснення генерації особистого та відкритого ключів ЕЦП заявник (підписувач, уповноважений представник) надає заявку адміністратору реєстрації АЦСК на електронному носії інформації. Якщо генерація особистого та відкритого ключа ЕЦП була проведена за межами АЦСК, адміністратор реєстрації проводить перевірку належності особистого ключа ЕЦП підписувачу та його відповідність відкритому ключу ЕЦП відповідно до п. 5.1. цього Регламенту.

Отримавши від заявника (підписувача, уповноваженого представника) заявку, адміністратор реєстрації перевіряє її, підписує своїм ЕЦП, зашифровує та надсилає засобами

телекомунікаційного зв’язку до АЦСК. Опрацювання заявки здійснюється протягом одного робочого дня з моменту її надходження до АЦСК.

6.2. Порядок формування сертифіката

Процедура формування сертифіката виконується АЦСК на підставі заявки, а також відомостей, отриманих від підписувача при проведенні процедури реєстрації.

Сформована заявка, що містить реєстраційні дані підписувача, відкритий ключ, інформацію про строк дії та іншу інформацію, що повинна бути включена до сертифіката, після успішного проходження процедури реєстрації підписується ЕЦП адміністратора реєстрації АЦСК та передається до АЦСК для сертифікації.

Після формування сертифікат, за згодою підписувача, може бути опублікований на сайті АЦСК. Інформація про дозвіл чи заборону публікації сертифіката вказується підписувачем в заявці.

Адміністратор реєстрації, за бажанням заявника:

- записує сформовані сертифікати на носій інформації та передає його заявнику;
- надає сертифікат - документ у паперовій формі, який засвідчуються печаткою АЦСК та власноручним підписом адміністратора реєстрації.

Після отримання сертифіката підписувач повинен перевірити достовірність відомостей, що в ньому містяться. При виявленні недостовірних даних підписувач повинен повідомити АЦСК (ВПР) у порядку, встановленому для скасування сертифіката. В такому випадку сертифікат скасовується та формується новий сертифікат ключа.

Якщо результати перевірки сформованого сертифіката позитивні, підписувач (заявник) визнає свій сертифікат шляхом засвідчення сертифіката в паперовій формі власноручним підписом або шляхом підписання акту виконаних робіт. У випадках, коли неможлива особиста присутність підписувача (заявника), його може представляти довірена особа – представник, яка разом з тим може засвідчити визнання сертифіката замість підписувача (заявника) своїм власноручним підписом. У цьому випадку заявник видає представнику доручення (довіреність) відповідного зразка.

Термін чинності сертифіката вказаний в сертифікаті і не може перевищувати двох років.

6.3. Повторне формування сертифіката

Повторне формування сертифіката – формування нового сертифіката для підписувача, який є власником чинного сертифіката, сформованого АЦСК.

Повторне формування сертифіката ключа може бути плановим та позаплановим.

Планове повторне формування сертифіката полягає у формуванні сертифіката на новий термін дії (після закінчення дії попередніх сертифікатів) до закінчення чинності попередніх сертифікатів.

Позапланове повторне формування сертифіката полягає у формуванні нового сертифіката підписувача у разі передчасного (протягом дії раніше виданого сертифіката) скасування чинного сертифіката, через компрометацію відповідного особистого ключа або зміну відомостей про підписувача, що зазначені у сертифікаті.

При повторному формуванні сертифіката АЦСК здійснює перевірку чинності інформації, яка надавалася раніше заявником під час реєстрації. Якщо дані, які надав заявник під час реєстрації, не змінились і порядок проведення процедури реєстрації заявників, передбачений цим Регламентом та чинним законодавством України, на час повторного звернення заявника (підписувача, уповноваженого представника) не було змінено, АЦСК залишає за собою право

зберігати в архіві тільки ті документи, які підтверджують відповідні зміни відомостей про підписувача (заявника), що зазначалися в сертифікаті.

6.4. Використання сертифіката та особистого ключа підписувача

АЦСК здійснює обслуговування сертифіката відповідно до договору.

Під час використання особистого ключа та сертифіката підписувач несе відповідальність за дії, що суперечать чинному законодавству України, цьому Регламенту та договору, що укладений між АЦСК та заявником. Користувач несе відповідальність під час використання сертифіката за дії, що суперечать чинному законодавству України та цьому Регламенту.

6.4.1. Обов'язки підписувача

Під час звернення до АЦСК або ВПР для формування сертифіката, а також при використанні сертифіката та особистого ключа, підписувачі зобов'язані:

- перед укладанням договору ознайомитись із Правилами, цим Регламентом та нормативно-правовими актами, що наведені в п.1;
- виконувати вимоги, передбачені договором, цим Регламентом та чинним законодавством України;
- надавати повні, достовірні відомості та іншу інформацію відповідно до договору, цього Регламенту та чинного законодавства України;
- надавати повну, достовірну інформацію, яка має бути включена до сертифіката, під час проходження процедури реєстрації в АЦСК або його ВПР, подавши належним чином оформлені документи, перелік яких розміщений на сайті АЦСК;
- своєчасно та в повному обсязі проводити розрахунки за послуги ЕЦП, що становлять предмет договору;
- додержуватись вимог щодо використання особистих ключів, визначених цим Регламентом та договором;
- зберігати особистий ключ в таємниці, вживати заходів щодо запобігання його втрати, розкриттю та несанкціонованому використанню;
- використовувати особистий ключ тільки в межах своїх повноважень;
- не розголошувати та не повідомляти іншим особам пароль доступу до особистого ключа та фразу-пароль для голосової автентифікації;
- використовувати надійні засоби ЕЦП для генерації особистих та відкритих ключів, формування та перевірки ЕЦП;
- перевіряти відповідність отриманого сертифіката до поданої заявки;
- не використовувати особистий ключ у разі його компрометації;
- негайно інформувати АЦСК про наступні події, якщо вони трапилися до закінчення строку чинності сертифікатів:
  - втрату або компрометацію особистого ключа;
  - втрату контролю щодо ключа через компрометацію пароля;
  - виявлення у сертифікаті неточностей або відомостей, що не відповідають дійсності;
  - зміну даних, що зазначені у сертифікатах.
- при виявленні неточностей або зміні даних, зазначених у сертифікаті, відкликати цей сертифікат;

- не використовувати особистий ключ після подання заяви на скасування чи блокування сертифіката;
- не використовувати особистий ключ відповідного сертифіката, що скасований або блокований.

Відповідальність за конфіденційність та цілісність особистого ключа несе підписувач.

6.4.2. Права підписувача

Під час звернення до АЦСК або ВПР для формування сертифіката, а також при використанні сертифіката та особистого ключа, підписувач має право:

- ознайомитись з інформацією щодо діяльності АЦСК в сфері надання послуг ЕЦП;
- отримати консультації з питань щодо створення, перевірки та використання ЕЦП, засобів генерації особистого та відкритого ключів, а також створення заявок на формування та зміну статусу сертифіката в АЦСК або його ВПР;
- генерувати в АЦСК або на своєму робочому місці відкриті та особисті ключі;
- отримувати сертифікат АЦСК;
- обумовити публікацію свого сертифіката на сайті АЦСК;
- отримувати повідомлення щодо зміни статусу свого сертифіката;
- отримувати списки відкликаних сертифікатів, які формує АЦСК;
- використовувати сертифікат АЦСК для перевірки чинності ЕЦП сертифікатів, які сформовані АЦСК;
- використовувати списки відкликаних сертифікатів, сформовані АЦСК, для перевірки як статусу власного сертифіката, так і сертифікатів інших підписувачів;
- подавати до АЦСК заяви, скарги, претензії тощо;
- надсилати заяви на скасування, блокування або поновлення свого сертифіката ключа у випадках, передбачених цим Регламентом та чинним законодавством України.

6.4.3. Обов’язки користувача

Перед використанням сертифіката, який був сформований АЦСК, користувач зобов’язаний:

- перевірити статус сертифіката за актуальним списком відкликаних сертифікатів або за протоколом визначення статусу сертифіката у режимі реального часу (OCSP);
- перевірити автентичність і цілісність списку відкликаних сертифікатів або відповіді сервера OCSP за допомогою відповідного сертифіката;
- використовувати сертифікат АЦСК для перевірки чинності ЕЦП сертифікатів, які сформовані АЦСК;

Якщо одержати інформацію про поточний стан сертифіката тимчасово неможливо, користувач повинен тимчасово відмовитись від використання сертифіката.

6.5. Скасування сертифікатів

Скасування сертифіката є достроковим припиненням його чинності. Скасовані сертифікати поновленню не підлягають.

Підписувач не має права використовувати для накладання ЕЦП особистий ключ, сертифікат якого скасований.

У випадку, якщо необхідне термінове припинення чинності сертифіката через об’єктивні обставини, з метою недопущення спричинення майнової шкоди, заявник (підписувач) має право заблокувати сертифікат за заявою в усній формі, а потім подати відповідну письмову заяву про скасування сертифіката.

6.5.1. Підстави для скасування сертифікатів

АЦСК негайно скасовує сформований ним сертифікат у разі:

- отримання від заявника (підписувача) або його уповноваженого представника заяви на скасування сертифіката;
- компрометації відповідного особистого ключа;
- смерті підписувача або оголошення його померлим за рішенням суду;
- визнання підписувача недієздатним за рішенням суду;
- припинення діяльності суб’єкта господарювання, реквізити якого зазначені в сертифікаті підписувача;
- виявлення факту надання підписувачем недостовірних даних;
- виявлення факту порушень вимог законодавства та цього Регламенту під час формування сертифіката;
- набрання законної сили рішенням суду про скасування сертифіката;
- розірвання підписувачем трудового договору або аналогічного документу, укладеного між підписувачем та роботодавцем — суб’єктом господарювання, реквізити якого зазначені в сертифікаті ключа підписувача;
- непоновлення підписувачем заблокованого сертифікату ключа протягом 90 календарних днів;
- припинення (розірвання) відповідного договору про надання послуг електронного цифрового підпису;
- в інших випадках, передбачених договором та чинним законодавством України.

6.5.2. Обставини, за яких сертифікат ключа повинен бути скасований підписувачем

Підписувач зобов’язаний звернутися до АЦСК (ВПР) для скасування сертифіката у разі:

– компрометації особистого ключа (факт або обґрунтована підозра того, що особистий ключ став відомий іншим особам, втрата можливості подальшого використання особистого ключа, зокрема, втрата або пошкодження носія ключової інформації тощо);

– зміни відомостей, що зазначені у сертифікаті;

– виявлення помилок у реквізитах сертифіката тощо.

6.5.3. Порядок скасування сертифікатів

Скасування сертифіката можуть ініціювати:

– підписувач;

– заявник;

– посадова особа АЦСК, яка має відповідні повноваження.

Скасування здійснюється на підставі заяви заявника чи підписувача, яка подана в письмовій формі, заяви підписувача, що має вигляд електронного документа, або за рішенням посадової особи АЦСК, що має на це відповідні повноваження.

Заява на скасування містить у собі наступні обов'язкові реквізити:

- ідентифікаційні дані;
- серійний номер сертифіката, що скасовується;
- причина скасування сертифіката;
- дата та підпис підписувача, заявника або його уповноваженого представника, відбиток печатки заявника (якщо заява подана заявником і заявник має печатку), а для заяви в електронній формі – ЕЦП підписувача.

Розгляд та опрацювання заяви на скасування сертифіката, інформування заявника (підписувача) про скасування здійснюється протягом двох годин з моменту надходження заяви до АЦСК (ВПР).

Часом скасування сертифіката встановлюється час зміни статусу сертифіката у реєстрі сертифікатів АЦСК.

6.5.3.1. Скасування сертифіката за заявою у письмовій формі

Для скасування сертифіката заявник або підписувач зобов'язаний подати до АЦСК або ВПР письмову заяву встановленого зразка, засвідчену особистим підписом підписувача або особистим підписом заявника та печаткою (якщо заявник має печатку).

6.5.3.2. Скасування сертифіката за заявою в електронній формі

Електронна заява подається до АЦСК або ВПР за встановленою формою та засвідчується ЕЦП підписувача. Заяви приймаються на електронну адресу, вказану на сайті АЦСК.

6.6. Блокування сертифікатів

Блокування сертифіката - це тимчасове припинення його чинності.

Підписувач не має права використовувати для накладення ЕЦП особистий ключ, сертифікат якого заблоковано.

АЦСК має право блокувати сертифікат з подальшим його скасуванням у випадку несплати послуг АЦСК відповідно до договору надання послуг.

6.6.1. Підстави для блокування сертифікатів

АЦСК негайно блокує сформований ним сертифікат у разі:

- отримання від заявника (підписувача) або його уповноваженого представника заяви на блокування сертифіката;
- підозри на компрометацію відповідного особистого ключа;
- набрання законної сили рішенням суду про блокування сертифіката;
- в інших випадках, передбачених договором та чинним законодавством України.

6.6.2. Порядок блокування сертифікатів

Блокування сертифіката можуть ініціювати:

– підписувач;

– заявник;

– посадова особа АЦСК, яка має відповідні повноваження.

Блокування сертифіката ключа підписувачем або заявником здійснюється на підставі заяви, яка подана в усній, письмовій формі чи у вигляді електронного документа.

Розгляд та опрацювання заяви на блокування сертифіката, інформування заявника (підписувача) про блокування здійснюється протягом двох годин з моменту надходження заяви до АЦСК (ВПР).

Часом блокування сертифіката встановлюється час зміни статусу сертифіката у реєстрі сертифікатів АЦСК.

Після блокування сертифіката заявник зобов'язаний протягом 90 календарних днів поновити чинність сертифіката або подати заяву про його скасування. У випадку, якщо протягом зазначеного терміну заявник не поновить чинність заблокованого сертифіката або не подасть заяви про його скасування, сертифікат автоматично скасовується АЦСК.

6.6.2.1. Блокування сертифіката за заявою в усній формі

Заява в усній формі подається до АЦСК (ВПР) в телефонному режимі за номером, який опублікований на сайті АЦСК. Для блокування заявник (підписувач) повинен повідомити співробітнику АЦСК (ВПР) наступну інформацію:

- ідентифікаційні дані власника сертифіката;
- серійний номер сертифіката;
- фраза-пароль для голосової автентифікації.

Заява в усній формі приймається тільки у випадку позитивної автентифікації (збігу фрази–пароля та ідентифікаційних даних підписувача з інформацією, вказаною в заявці).

Прийняття і обробка усних заяв на блокування сертифікатів здійснюється цілодобово.

6.6.2.2. Блокування сертифіката за заявою в електронній формі

Електронна заява на блокування має встановлену форму та засвідчується ЕЦП підписувача.

Електронна заява на блокування підписується власником сертифіката за допомогою надійних засобів ЕЦП і подається до АЦСК або ВПР засобами телекомунікаційного зв'язку на електронну адресу, вказану на сайті АЦСК.

6.6.2.3. Блокування сертифіката за заявою у письмовій формі

Письмова заява на блокування сертифіката подається до АЦСК або ВПР за встановленою формою.

Письмова заява на блокування сертифіката засвідчується особистим підписом підписувача або особистим підписом заявника та печаткою (якщо заявник має печатку).

6.7. Поновлення сертифікатів

Поновлення сертифіката можливе лише для заблокованих сертифікатів, термін блокування яких не закінчився. Скасовані сертифікати поновленню не підлягають.

6.7.1. Підстави для поновлення сертифікатів

АЦСК поновлює заблокований сертифікат у разі:

- отримання від заявника (підписувача) або його уповноваженого представника заяви на поновлення сертифіката;
- встановлення недостовірності відомостей про компрометацію відповідного особистого ключа;
- набрання законної сили рішенням суду про поновлення сертифіката;
- в інших випадках, передбачених договором та чинним законодавством України.

6.7.2. Порядок поновлення сертифікатів

Поновлення заблокованого сертифіката можуть ініціювати:

– підписувач;

– заявник;

– посадова особа АЦСК, яка має відповідні повноваження.

Для поновлення чинності сертифіката підписувач або заявник подає до АЦСК чи ВПР письмову заяву встановленого зразка. Заява про поновлення чинності сертифіката засвідчується особистим підписом підписувача або особистим підписом заявника та печаткою (якщо заявник має печатку).

Опрацювання письмової заяви на поновлення чинності сертифіката, її розгляд та інформування заявника (підписувача) про поновлення здійснюється протягом двох годин з моменту надходження заяви до АЦСК.

Часом поновлення чинності сертифіката вважається час зміни його статусу у реєстрі сертифікатів АЦСК.

6.8. Розповсюдження інформації про статус сертифікатів

Для розповсюдження інформації про статус сертифікатів використовується механізм списків відкликаних сертифікатів та механізм визначення статусу сертифіката в режимі реального часу за протоколом OCSP.

Списки відкликаних сертифікатів оновлюються та публікуються відповідно до п.4.4 цього Регламенту.

АЦСК надає всім користувачам послугу інтерактивного визначення статусу сертифіката за протоколом OCSP. Послуга надається шляхом відправлення запиту на OCSP-сервер АЦСК. Сформовані відповіді, що містять інформацію про статус сертифіката, засвідчуються ЕЦП OCSP-сервера. Формат запиту на OCSP-сервер АЦСК та відповіді OCSP-сервера відповідає вимогам спільного наказу Міністерства юстиції України та Адміністрації Держспецзв'язку від 20.08.2012 № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису».

Послуга інтерактивного визначення статусу сертифіката надається цілодобово.

6.9. Закінчення строку чинності сертифіката підписувача

Після закінчення терміну дії сертифіката він позначається в реєстрі сертифікатів як скасований, вилучається з інформаційного ресурсу АЦСК та переміщується в архів. АЦСК зберігає сертифікат та пов'язану з ним інформацію про його статус безстроково.

За запитом користувача, що надсилається за протоколом OCSP, АЦСК надає доступ до необхідного сертифіката та інформацію про його статус.

6.10. Порядок надання послуги фіксування часу

Позначка часу - сукупність електронних даних, створена за допомогою технічних засобів ПТК АЦСК, яка підтверджує наявність електронного документа (електронних даних) на певний момент часу.

Послуга фіксування часу - процедура засвідчення наявності електронного документа (електронних даних) на певний момент часу шляхом додання до нього або логічного поєднання з ним позначки часу.

АЦСК надає всім користувачам послугу фіксування часу. Послуга надається шляхом відправлення запиту на TSP-сервер АЦСК. Сформовані позначки часу засвідчуються ЕЦП TSP-сервера. Формат запиту на TSP-сервер АЦСК та відповіді TSP-сервера відповідає RFC 3161.

Послуга фіксування часу надається цілодобово.

7. Управління та операційний контроль

7.1. Фізичне середовище

7.1.1. Приміщення АЦСК

Приміщення АЦСК розташоване в орендованій частині другого поверху нежилого будинку за адресою: 04080, м. Київ, вул. Фрунзе, 102.

Приміщення АЦСК складається із трьох зон:

- спеціальне приміщення, в якому розташована екранована шафа;
- приміщення архіву;
- адміністративні приміщення.

Вхідні двері АЦСК стійкі до злому, обладнані механічним та електромагнітним замками.

Ключі від приміщень АЦСК мають відповідальні особи, які у неробочий час передають під охорону приміщення АЦСК. Дублікати ключів від робочих приміщень АЦСК зберігаються у сейфі адміністратора безпеки АЦСК.

Безпека інформаційних ресурсів в АЦСК досягається шляхом впровадження організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації комплексної системи захисту інформації.

Всі приміщення обладнані системою контролю доступу, охоронною та пожежною сигналізацією.

Обладнання ПТК, що забезпечує формування сертифікатів, управління статусом сертифікатів та зберігання особистих ключів АЦСК, розміщується в екранованій шафі, яка знаходиться в спеціальному приміщенні.

Екранована шафа забезпечує пасивний захист інформації від витоку каналами ПЕМВН, від порушення її цілісності внаслідок деструктивного впливу зовнішніх електромагнітних полів. Величина ефективності екранування екранованої шафи відповідає встановленим нормам.

Для заземлення екранованої шафи та обладнання спеціального приміщення влаштований окремий контур заземлення. Електроживлення вводиться в екрановану шафу через

протизавадні фільтри. Підключення серверів АЦСК, що розміщені у спеціальному приміщенні, виконане через волоконно-оптичні лінії зв'язку.

В АЦСК реалізовано адміністрування з метою розмежування доступу обслуговуючого персоналу до ресурсів системи. Доступ надається тільки після успішної авторизації обслуговуючого персоналу (можливість виконувати тільки ті функції, що доступні та асоційовані з їх ролями).

7.1.2. Пропускний і внутрішній режим

Пропускний і внутрішній режим передбачає порядок допуску співробітників і представників інших організацій на територію АЦСК, порядок внесення і винесення матеріальних цінностей, а також виконання особами, що перебувають на території АЦСК, встановлених вимог режиму і розпорядку робочого дня.

Допуск у спеціальне приміщення у режимі штатної роботи АЦСК мають:

- керівник ЦСК;
- заступник керівника АЦСК;
- адміністратор безпеки;
- адміністратор сертифікації;
- системний адміністратор.

Інші особи мають право доступу до спеціального приміщення тільки в супроводі адміністратора безпеки, керівника АЦСК або його заступника.

Допуск у приміщення архіву у режимі штатної роботи АЦСК мають:

- керівник ЦСК;
- заступник керівника АЦСК;
- адміністратор безпеки;
- архіваріус.

Інші особи мають право доступу до приміщення архіву тільки в супроводі адміністратора безпеки, керівника АЦСК або його заступника.

Контроль за організацією охорони, станом пропускного й внутрішнього режиму здійснює адміністратор безпеки АЦСК.

Особи, що порушують пропускний і внутрішній режим, притягуються до дисциплінарної відповідальності.

7.2. Процедурний контроль

7.2.1. Права, обов'язки та відповідальність АЦСК

7.2.1.1. Права АЦСК

АЦСК під час формування та обслуговування сертифікатів має право:

- надавати послуги ЕЦП та обслуговувати сертифікати відповідно до вимог законодавства України;
- вимагати, отримувати та перевіряти інформацію, необхідну для реєстрації заявника і формування сертифіката, безпосередньо у заявника (юридичної або фізичної особи) або її уповноваженого представника;

- не приймати заявки у тому випадку, якщо формати даних, створені засобом КЗІ, яким користувався заявник для формування заявок, не підтримуються АЦСК;
- блокувати, скасовувати, поновлювати сертифікати у порядку, встановленому Правилами та цим Регламентом;
- вимагати від підписувача (заявника) дотримання вимог Регламенту, умов договору;
- припиняти надання послуг ЕЦП за умов порушення вимог договору або цього Регламенту.

7.2.1.2. Обов'язки АЦСК

АЦСК під час формування та обслуговування сертифікатів зобов'язаний:

- під час реєстрації встановлювати заявника відповідно до вимог, визначених в цьому Регламенті та законодавстві України, у тому числі встановлювати належність відповідного особистого ключа заявнику, якщо генерація ключів здійснювалося не в АЦСК або ВПР;
- формувати посилений сертифікат відкритого ключа;
- забезпечувати унікальність реєстраційного номера сертифіката, який формується АЦСК;
- скасовувати та блокувати сертифікати у порядку, визначеному цим Регламентом, формувати списки відкликаних сертифікатів;
- поновлювати сертифікати відповідно до порядку, що визначений цим Регламентом;
- зберігати документи, на підставі яких були сформовані, скасовані, заблоковані та поновлені сертифікати протягом терміну, що передбачений цим Регламентом;
- забезпечувати надійне збереження сформованих сертифікатів та документів, що надавалися заявником для реєстрації;
- публікувати список відкликаних сертифікатів на сайті АЦСК;
- забезпечувати можливість цілодобового вільного доступу користувачів до сертифікатів АЦСК, сертифікатів підписувачів (за згоди їх власників), даних про статус сертифікатів;
- використовувати для надання послуг ЕЦП ПТК, засоби КЗІ, в тому числі засоби ЕЦП, що мають позитивний експертний висновок за результатами державної експертизи у сфері КЗІ;
- забезпечувати розташування засобів ПТК в спеціально обладнаних приміщеннях, їх охорону з метою запобігання незаконному проникненню сторонніх осіб в приміщення АЦСК;
- забезпечувати надійний захист персональних даних, отриманих від підписувача, та інформації в АС згідно з чинним законодавством;
- інформувати користувачів про необхідність перевірки чинності сертифіката перед його використанням;
- цілодобово приймати заяви підписувачів про скасування, блокування та поновлення сертифікатів ключів.

7.2.1.3. Відповідальність АЦСК

АЦСК під час формування та обслуговування сертифікатів несе відповідальність за:

- внесення у сертифікат відомостей, відмінних від тих, що вказані у заявці;
- порушення вимог Правил та/або Регламенту під час встановлення заявника;
- несвоєчасну публікацію списків відкликаних сертифікатів;
- помилкове відкликання або блокування сертифікатів;
- компрометацію особистого ключа АЦСК;
- відмову та збої технічних і програмних засобів ПТК;
- помилкові та/або протиправні дії обслуговуючого персоналу АЦСК;
- захист персональних даних підписувачів.

7.2.2. Склад організаційної структури АЦСК

До складу організаційної структури АЦСК, задіяної в обслуговуванні сертифікатів ключів, входять такі підрозділи та посади:

- адміністрація:
  - керівник АЦСК;
  - заступник керівника АЦСК;
- відділ сертифікації:
  - адміністратор сертифікації;
- відділ реєстрації:
  - адміністратор реєстрації;
- архівний відділ:
  - архіваріус;
- служба захисту інформації:
  - адміністратор безпеки;
  - системний адміністратор;
- ВПР (за наявності):
  - адміністратор реєстрації.

Обов’язки та відповідальність посадових осіб АЦСК визначається відповідними посадовими інструкціями.

Організаційна структура АЦСК може бути розширена шляхом введення до складу АЦСК додаткових підрозділів та посад.

7.2.2.1. Адміністрація

Функції та завдання адміністрації:

- визначення основних шляхів розвитку, координація, регламентування, контроль та аналіз діяльності;
- забезпечення структурних підрозділів АЦСК необхідними ресурсами для досягнення визначених цілей;
- контроль за виконанням зауважень, пропозицій та вимог заявників і підписувачів, направлених на удосконалення роботи АЦСК.

7.2.2.2. Відділ сертифікації

До складу відділу сертифікації входять адміністратори сертифікації.

Адміністратор сертифікації:

- подає до центрального засвідчувального органу дані, необхідні для формування сертифіката та засвідчення відкритого ключа АЦСК;
- відповідає за формування, скасування, блокування та поновлення сертифікатів;
- відповідає за використання особистого ключа АЦСК під час формування сертифікатів та списків відкликаних сертифікатів;
- забезпечує формування списків відкликаних сертифікатів та позначок часу;
- забезпечує ведення, архівацію та відновлення бази даних сформованих сертифікатів;
- забезпечує публікацію сертифікатів та списків відкликаних сертифікатів;
- інформує адміністратора безпеки про події, що впливають на безпеку функціонування акредитованого центру.

7.2.2.3. Відділ реєстрації

До складу відділу реєстрації входять адміністратори реєстрації.

Адміністратор реєстрації відповідає за:

- встановлення осіб, які звернулися до АЦСК для формування сертифіката;
- перевірку даних, обов'язкових для формування сертифіката, а також даних, які вносяться у сертифікат на вимогу підписувача;
- укладення договорів про надання послуг електронного цифрового підпису.
- отримання від заявників (підписувачів) заявок на формування, скасування, блокування та поновлення сертифікатів;
- передачу заявок на формування сертифіката до АЦСК;
- перевірку законності звернень щодо блокування, поновлення та скасування сертифікатів;
- надання консультацій підписувачам під час генерації ключів у разі отримання від них відповідного звернення;
- забезпечення конфіденційності ключової інформації під час генерації ключів підписувачів в АЦСК;
- надання консультацій підписувачам щодо умов та порядку надання послуг ЕЦП;
- інформування адміністратора безпеки про події, що впливають на безпеку функціонування акредитованого центру.

7.2.2.4. Архівний відділ

До складу архівного відділу входять архіваріуси.

Архіваріус:

- веде діловодство архіву: реєструє вхідні, вихідні документи та інше;
- приймає, перевіряє і реєструє комплекти документів, що надійшли до архіву, на підставі яких було сформовано сертифікати;

- систематизує і розміщує справи, веде їх облік, забезпечує зручний і швидкий їх пошук;
- здійснює облік укладених договорів про надання послуг ЕЦП в електронному вигляді;
- забезпечує упорядкування, комплектування, використання, збереження прийнятих в архів документів;
- забезпечує захист інформації персональних даних підписувачів;
- контролює додержання правил протипожежної безпеки в приміщеннях архіву;
- виконує інші функції, що випливають з покладених на архів завдань.

7.2.2.5. Служба захисту інформації

Склад служби захисту інформації визначається положенням про службу захисту інформації в АЦСК. До складу службу захисту інформації входять адміністратор безпеки та системний адміністратор.

Адміністратор безпеки відповідає за:

- забезпечення повноти та якісного виконання організаційно-технічних заходів із захисту інформації;
- розроблення розпорядчих документів, згідно з якими в АЦСК повинен забезпечуватися захист інформації, і контроль за їх виконанням;
- своєчасне реагування на спроби несанкціонованого доступу до ресурсів програмно-технічного комплексу АЦСК, порушення правил експлуатації засобів захисту інформації;
- контроль збереження особистих ключів АЦСК, серверів АЦСК та їх резервних копій, особистих ключів посадових осіб АЦСК;
- контроль знищення особистих ключів АЦСК, серверів АЦСК та посадових осіб;
- контроль процесу резервування сертифікатів та списків відкликаних сертифікатів, а також інших важливих ресурсів;
- організацію розмежування доступу до ресурсів програмно-технічного комплексу АЦСК, зокрема розподілення між посадовими особами паролів, ключів, сертифікатів тощо;
- спостереження за функціонуванням комплексної системи захисту інформації;
- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації після збоїв, відмов, аварій програмно-технічного комплексу;
- ведення журналу аудиту.

Системний адміністратор забезпечує:

- організацію експлуатації та технічного обслуговування програмно-технічного комплексу АЦСК;
- здійснення адміністрування сервера бази даних програмно-технічного комплексу;
- підтримку електронного інформаційного ресурсу, публікацію сертифікатів та списку відкликаних сертифікатів;
- адміністрування засобів програмно-технічного комплексу;
- участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації;

- встановлення та налагодження програмного забезпечення системи резервного копіювання бази даних програмно-технічного комплексу;
- формування та ведення резервних копій загальносистемного та спеціального програмного забезпечення програмно-технічного комплексу;
- актуальність еталонних, архівних і резервних копій баз сертифікатів та їх зберігання;
- ведення, архівацію та відновлення еталонної бази даних сформованих сертифікатів.

7.2.2.6. ВПР

До складу ВПР (в разі наявності ВПР) входить адміністратор реєстрації.

Адміністратор реєстрації ВПР відповідає за:

- встановлення осіб, які звернулися до ВПР для формування сертифіката;
- перевірку даних, обов'язкових для формування сертифіката, а також даних, які вносяться у сертифікат на вимогу підписувача;
- укладення договорів про надання послуг електронного цифрового підпису.
- отримання від заявників (підписувачів) заявок на формування, скасування, блокування та поновлення сертифікатів;
- передачу заявок на формування сертифіката до АЦСК;
- перевірку законності звернень щодо блокування, поновлення та скасування сертифікатів;
- надання консультацій підписувачам під час генерації ключів у разі отримання від них відповідного звернення;
- забезпечення конфіденційності ключової інформації під час генерації ключів підписувачів у ВПР;
- надання консультацій підписувачам щодо умов та порядку надання послуг ЕЦП;
- інформування адміністратора безпеки АЦСК про події, що впливають на безпеку функціонування ВПР.

7.3. Порядок ведення журналів аудиту АС АЦСК

ПТК АЦСК забезпечує реєстрацію у журналах аудиту АС АЦСК таких подій:

- спроб створення, знищення, встановлення пароля, зміни прав доступу, системних привілеїв тощо у ПТК;
- генерації та використання ключової інформації;
- формування, блокування, скасування та поновлення сертифікатів ключів, а також формування списків відкликаних сертифікатів;
- спроб несанкціонованого доступу до ПТК;
- надання доступу до ПТК персоналу АЦСК;
- збоїв у роботі ПТК.

ПТК АЦСК забезпечує реєстрацію у журналах аудиту АС ВПР таких подій:

- спроб створення, знищення, встановлення пароля, зміни прав доступу, системних привілеїв тощо у ПТК;
- генерації та використання ключової інформації;

– спроб несанкціонованого доступу до ПТК;

– збоїв у роботі ПТК.

Захист журналів аудиту АС забезпечується засобами ПТК, контроль за якими здійснюється адміністратором безпеки АЦСК.

Повний доступ до журналу аудиту має виключно адміністратор безпеки. Адміністратор сертифікації має право на читання (перегляд) змісту журналу.

Для всіх інших користувачів чинний журнал аудиту відкрито виключно на запис.

Усі записи в журналах аудиту в електронній або паперовій формі містять дату та час події, а також ідентифікаційну інформацію щодо суб'єкта, що ініціював цю подію.

Засобами ПТК заборонено модифікацію окремих записів чинного журналу аудиту. Записи захищаються від несанкціонованого видалення засобами системи управління базою. Очищення журналів аудиту виконується адміністратором безпеки тільки після створення резервної копії журналу в архіві.

Адміністратор безпеки періодично, але не рідше одного разу на добу, переглядає журнали аудиту з метою виявлення подій, які свідчать про ситуацію, що призвела або може призвести до порушення безпеки технічних засобів АЦСК.

7.4. Порядок ведення архівів та зберігання документованої інформації

Архівному зберіганню підлягають такі документи та дані АЦСК:

- сертифікати АЦСК;
- сертифікати серверів АЦСК;
- сертифікати посадових осіб АЦСК;
- сертифікати підписувачів АЦСК;
- заявки на сертифікацію;
- укладені договори про надання послуг електронного цифрового підпису;
- документи та копії документів, надані під час реєстрації заявника;
- заяви на зміну статусу сертифікатів (скасування, блокування, поновлення);
- сформовані позначки часу;
- службова інформація ПТК АЦСК;
- журнали аудиту АЦСК.

Документи АЦСК на паперових носіях зберігаються у відповідному приміщенні АЦСК, обладнаному системою контролю доступу, охоронною та пожежною сигналізацією. Дозволяється зберігання документів на паперових носіях у територіально віддаленому сховищі, доступ до якого мають адміністратор безпеки та керівник АЦСК.

Документи, що надавалися заявником для реєстрації, зберігаються протягом терміну дії відповідного сертифіката. Укладені договори про надання послуг ЕЦП зберігаються протягом терміну позовної давності.

Знищення архівних документів здійснюється комісією, до складу якої входять архіваріус, адміністратор сертифікації та адміністратор безпеки. По завершенні процедури знищення архівних документів складається відповідний акт, який затверджує керівник АЦСК.

Сертифікати АЦСК, серверів АЦСК, посадових осіб АЦСК та підписувачів, а також списки відкликаних сертифікатів в архівному режимі зберігаються безстроково.

Сформовані позначки часу зберігаються не менше одного року.

Засобами СКБД, що входять до складу ПТК, виконується автоматичне резервне копіювання БД АЦСК. Створення резервної копії засобами СКБД виконується раз на добу, під час найменшого завантаження серверу. Копіювання даних здійснюється на накопичувач на жорстких магнітних дисках, а потім на оптичний носій типу CD(DVD)-R(RW).

Після створення нової резервної копії, попередня резервна копія стає архівною.

Архівні копії журналів аудиту ПТК АЦСК зберігаються не менше трьох років.

Для зберігання носіїв інформації з резервними та архівними копіями виділяється окреме сховище (сейф) з двома екземплярами ключів і пристроями для опечатування замкових щілин. Один екземпляр ключа від сховища знаходиться в уповноваженої посадової особи АЦСК, яка відповідає за створення та зберігання резервних та архівних копій, а другий – в опечатаному вигляді зберігається у сховищі адміністратора безпеки АЦСК або керівника АЦСК.

Відповідальність за контроль автоматичного резервного копіювання та виконання резервного копіювання в ручному режимі покладається на системного адміністратора АЦСК. Адміністратор безпеки періодично контролює процес створення та зберігання резервних копій.

8. Управління ключами та забезпечення захисту особистого ключа АЦСК

8.1. Порядок генерації ключів підписувачів

Генерація особистих та відкритих ключів ЕЦП виконується при формуванні нового сертифіката, а також при плановій та позаплановій заміні особистого ключа підписувача.

Відкритий та особистий ключі підписувача можуть бути згенеровані:

- на робочій станції підписувача виключно з використанням надійних засобів ЕЦП;
- на робочій станції генерації ключів підписувачів в АЦСК або ВПР.

В процесі генерації ключів створюється особистий ключ та заявка на формування сертифіката. Заявка, що передається на сертифікацію до АЦСК, є самопідписаним запитом формату PKCS#10, який засвідчується ЕЦП за допомогою особистого ключа підписувача, що йому відповідає.

Під час обробки заявки здійснюється перевірка належності особистого ключа підписувача відкритому ключу, який міститься у заявці. Перевірка здійснюється програмним забезпеченням ПТК АЦСК автоматично, шляхом перевірки ЕЦП, накладеного на заявку, з використанням відкритого ключа, що міститься в заявці. Формування сертифіката можливе лише за умови успішної перевірки.

8.1.1. Генерація ключів на робочій станції підписувача

Особистий і відкритий ключі підписувача генеруються особисто підписувачем на його робочій станції із застосуванням надійних засобів ЕЦП. Генерація здійснюється з використанням технічних засобів підписувача. Особистий ключ підписувача захищається паролем.

По закінченні процедури генерації особистий ключ підписувача записується на електронний носій інформації та залишається у підписувача.

Відповідальність за забезпечення конфіденційності та цілісності особистого ключа під час генерації на робочій станції підписувача повністю несе підписувач.

Передача підписувачем сформованої заявки, що містить відкритий ключ, до АЦСК або ВПР здійснюється на носії інформації ним особисто або його довіреною особою.

8.1.2. Генерація ключів на робочій станції АЦСК

Особистий і відкритий ключі підписувача генеруються особисто підписувачем або його довіреною особою, що має відповідні повноваження, на робочій станції генерації ключів підписувачів, що входить до складу ПТК АЦСК . Особистий ключ підписувача захищається паролем.

Під час генерації ключів адміністратор реєстрації, за згодою підписувача або його довіреної особи, може надавати консультаційну допомогу щодо процесу генерації ключів.

По закінченні процедури генерації особистий ключ підписувача записується на носій ключової інформації, який залишається у підписувача (його довіреної особи), а відкритий ключ у складі заявки на формування сертифіката передається на службовому електронному носії інформації на робочу станцію адміністратора реєстрації.

Особисті ключі підписувачів не зберігаються в АЦСК.

Після генерації та запису особистого ключа підписувача на носій ключової інформації він автоматично знищується на станції генерації ключів способом, що не допускає його відновлення.

Генерація ключів довіреною особою заявника (підписувача) може здійснюватися лише під контролем адміністратора реєстрації з метою недопущення несанкціонованого копіювання особистого ключа довіреною особою на інші носії інформації або його несанкціонованої модифікації.

У випадку генерації ключів довіреною особою заявника (підписувача) носій ключової інформації вкладається у непрозорий конверт, який запечатується, скріплюється печаткою АЦСК, підписами довіреної особи та адміністратора реєстрації. Після передачі конверта з носієм ключової інформації довіреній особі заявника (підписувача) відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе заявник (підписувач).

У разі, якщо генерація ключів здійснювалась довіреною особою, підписувач (заявник) при отриманні від довіреної особи конверта з особистим ключем та паролем зобов’язаний виконати наступні дії:

- перевірити цілісність конверта;
- якщо цілісність не порушена, то невідкладно, перед першим використанням особистого ключа для накладання підпису, підписувач зобов’язаний змінити пароль доступу до нього;
- у разі, якщо неможливо змінити пароль шляхом перезапису ключа на той самий носій ключової інформації (наприклад, ключ записаний на носій CD-R), необхідно після зміни паролю зберегти особистий ключ на новому носії, а попередній носій особистого ключа знищити надійним способом, що не дозволяє його відновлення;
- при порушенні цілісності конверта, заявник (підписувач) невідкладно зобов’язаний звернутись до АЦСК із заявою про скасування сертифіката.

8.2. Порядок генерації та захисту особистих ключів АЦСК

Генерація особистих ключів АЦСК та серверів АЦСК здійснюється за допомогою засобів ПТК АЦСК у спеціальному приміщенні двома адміністраторами сертифікації під контролем адміністратора безпеки.

Кожен згенерований особистий ключ АЦСК або сервера АЦСК записується у БД ПТК АЦСК з розподілом таємниці на дві частини, кожна з яких захищається паролем відповідного адміністратора сертифікації. Захист особистого ключа під час запису до БД виконується

відповідно до методики зберігання особистого ключа АЦСК, погодженої з Адміністрацією Держспецзв'язку.

Запит на формування сертифіката АЦСК або сервера АЦСК, що містить відкритий ключ, записується на локальний диск сервера АЦСК для подальшого формування сертифіката.

Після закінчення процедури генерації ключів запит на формування сертифіката АЦСК, що містить відкритий ключ, записується на змінний носій та передається адміністратором сертифікації у ЦЗО.

Формування сертифікатів серверів АЦСК виконується на сервері АЦСК в спеціальному приміщенні адміністратором сертифікації у присутності адміністратора безпеки на основі попередньо сформованих запитів. Сформовані сертифікати серверів записуються в БД ПТК АЦСК.

Адміністратори сертифікації можуть надати доступ до особистого ключа АЦСК або сервера АЦСК будь-якій кількості нових адміністраторів. Для цього два адміністратори, що брали участь у генерації ключа, відновлюють особистий ключ, після чого нові адміністратори створюють свої частини розділеної таємниці, захищені їх особистими паролями.

Таким чином, в результаті будь-які два адміністратори сертифікації можуть після автентифікації в ПТК АЦСК отримати доступ до особистого ключа ЦСК або сервера ЦСК, але жоден з адміністраторів не може відновити особистий ключ самостійно.

8.3. Порядок резервування та відновлення особистих ключів АЦСК

Резервна копія таблиці БД ПТК АЦСК, що містить ключову інформацію в зашифрованому вигляді, створюється наступним чином:

- системний адміністратор засобами СКБД створює дамп даних;
- системний адміністратор створює архів дампа за допомогою архіватора.

Архів записується в двох екземплярах на CD(DVD)-R. На носіях CD(DVD)-R робиться напис із зазначенням номеру носія та дати запису на нього резервної копії.

Резервна копія зберігається у спеціальному приміщенні АЦСК.

Всі події реєструються у журналі обліку резервних копій даних.

Резервна копія створюється кожного разу після таких подій:

- генерація особистих ключів АЦСК або серверів АЦСК;
- створення або видалення облікових записів адміністраторів сертифікації.

При створенні нової резервної копії попередня копія знищується способом, що не допускає її відновлення.

Паролі адміністраторів сертифікації, необхідні для відновлення особистих ключів, разом з іншою ідентифікаційною інформацією (паролі доступу до операційних систем, систем управління базами даних, тощо) зберігаються в сейфі адміністратора безпеки АЦСК. Дані кожного адміністратора знаходяться в окремому конверті, на який накладено особистий підпис адміністратора.

У випадку втрати чи пошкодження ключової інформації та неможливості відновити її стандартними засобами СКБД використовується резервна копія ключових даних. Адміністратор сертифікації під контролем адміністратора безпеки імпортує дані з файлів резервної копії до БД.

8.4. Протоколювання операцій з особистим ключем АЦСК

Будь-яка операція з особистим ключем АЦСК або сервера АЦСК протоколюється в електронному або паперовому журналі із зазначенням дати та часу здійснення операції, типу операції, ідентифікатора посадової особи АЦСК, що виконала операцію.

8.5. Строки дії особистих ключів АЦСК та порядок їх заміни

Максимальний строк дії ключів АЦСК не може перевищувати п’яти років, ключів серверів АЦСК та уповноважених посадових осіб АЦСК — двох років.

Початком строку дії особистого ключа АЦСК або посадової особи АЦСК вважається дата та час початку строку дії відповідного сертифіката АЦСК, сервера або посадової особи АЦСК.

Після закінчення терміну дії особистий ключ та всі його резервні копії знищуються способом, що не дозволяє їх відновлення.

8.5.1. Порядок планової зміни ключів АЦСК та посадових осіб АЦСК

Планова зміна ключів АЦСК виконується тоді, коли до закінчення терміну дії особистого ключа залишається не менше двох років. Планова зміна ключів серверів АЦСК та посадових осіб АЦСК виконується по закінченню їх терміну дії.

Планова заміна ключів уповноваженої посадової особи АЦСК здійснюється не частіше одного разу на рік та не пізніше ніж через 2 (два) роки після початку дії особистого ключа уповноваженої посадової особи АЦСК.

Процедура планової зміни ключів АЦСК та серверів АЦСК здійснюється в такому порядку:

- двоє адміністраторів сертифікації в присутності адміністратора безпеки виконують генерацію нового особистого ключа АЦСК або сервера АЦСК;
- адміністратор сертифікації ініціює процес засвідчення чинності відкритого ключа АЦСК в ЦЗО або формує новий сертифікат сервера АЦСК;
- після отримання сертифіката АЦСК від ЦЗО або після формування сертифіката сервера АЦСК, новий сертифікат публікується на сайті АЦСК.

Після планової заміни старий особистий ключ АЦСК використовується для підпису відповідних списків відкликаних сертифікатів до завершення терміну дії останнього підписаного ним сертифіката підписувача, після чого знищується надійним способом.

Старий особистий ключ сервера АЦСК після планової заміни знищується надійним способом.

Старий сертифікат АЦСК використовується для перевірки ЕЦП на раніше сформованих сертифікатах ключів та списках відкликаних сертифікатів.

Старий сертифікат сервера АЦСК використовується для перевірки ЕЦП на раніше сформованих повідомленнях (позначках часу, інформації про статус сертифіката тощо).

Процедура планової заміни ключів уповноважених посадових осіб АЦСК здійснюється в наступному порядку:

- уповноважена посадова особа АЦСК генерує новий особистий ключ та відповідну йому заявку на формування сертифіката;
- адміністратор сертифікації або уповноважена посадова особа АЦСК виготовляє новий сертифікат ключа посадової особи АЦСК;
- старий особистий ключ посадової особи АЦСК знищується надійним способом, а старий сертифікат ключа скасовується.

Перевірка ЕЦП на документах, підписаних за допомогою старого особистого ключа посадової особи, здійснюється шляхом застосування відповідного йому скасованого сертифікату ключа, який зберігається в реєстрі сертифікатів ключів АЦСК.

8.5.2. Порядок позапланової зміни ключів АЦСК

У випадку компрометації або загрози компрометації особистого ключа АЦСК, сервера АЦСК або посадових осіб АЦСК виконується позапланова зміна ключів.

АЦСК негайно сповіщає ЦЗО про факт компрометації особистого ключа АЦСК з метою його скасування шляхом внесення до списку відкликаних сертифікатів.

Процедура позапланової зміни ключів АЦСК та серверів АЦСК виконується у порядку, визначеному процедурою планової зміни ключів.

У випадку компрометації особистого ключа АЦСК сертифікати всіх підписувачів скасовуються. Усі сертифікати підписувачів, що діяли на момент компрометації ключа АЦСК, а також сертифікати, які були заблоковані, повинні бути позапланово замінені. Списки відкликаних сертифікатів підписуються новим особистим ключем АЦСК.

Після публікації нового сертифіката на сайті АЦСК старий особистий ключ знищується надійним способом.

АЦСК офіційно сповіщає заявників про факт позапланової заміни ключів АЦСК. Після одержання офіційного повідомлення про факт позапланової заміни ключів АЦСК заявникам необхідно виконати процедуру одержання нових сертифікатів відповідно до положень цього Регламенту.

У випадку компрометації особистого ключа уповноваженої посадової особи АЦСК сертифікат уповноваженої посадової особи АЦСК скасовується.

Після скасування сертифікату ключа уповноваженої посадової особи АЦСК виконується процедура позапланової заміни ключів уповноваженої посадової особи АЦСК. Процедура позапланової заміни ключів виконується в порядку, визначеному у процедурі планової заміни ключів уповноваженої посадової особи АЦСК.