

Затверджую  
 Директор ТОВ «Український  
 сертифікаційний центр»  
  
 Шаталов О.С.  
 «06» 07 2009 року.

## КОМЕНТАР ДО РЕГЛАМЕНТУ АЦСК «УКРАЇНСЬКИЙ СЕРТИФІКАЦІЙНИЙ ЦЕНТР»

*Редакція від 02.07.2009р.*

*Цей коментар складено на виконання статті Закону України «Про електронний цифровий підпис» в частині надання своїм дійсним та потенційним клієнтам консультацій в частині застосування електронного цифрового підпису в Україні.*

### 3.3 Обмеження щодо використання сертифікатів

**ЦСК не встановлює обмеження щодо використання сформованих ним сертифікатів.**

*Сертифікати використовуються в рамках діючого законодавства. Обмеження на використання встановлено:*

- *Законом України «Про електронні документи та електронний документообіг»*  
**Стаття 8. Правовий статус електронного документа та його копії**  
*Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.*  
*Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму.*  
*Електронний документ не може бути застосовано як оригінал:*
  - 1) *свідоцтва про право на спадщину;*
  - 2) *документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів;*
  - 3) *в інших випадках, передбачених законом.**Нотаріальне посвідчення цивільно-правової угоди, укладеної шляхом створення електронного документа (електронних документів), здійснюється у порядку, встановленому законом.*
- *Постановою Кабінету Міністрів України від 28 жовтня 2004 р. N 1452в*  
*п. 4. Установа не застосовує електронний цифровий підпис:*
  - *для складання електронних документів, які не можуть бути*
  - *оригіналами у випадках, передбачених законодавством;*
  - *для вчинення правочинів на суму, що перевищує 1 млн. гривень.*
- *Іншими законодавчими та підзаконними актами.*

### 4.5 Порядок публікації списку відкликаних сертифікатів

**Список відкликаних сертифікатів на інформаційному ресурсі ЦСК публікується одразу після його формування.**

**ЦСК формує повний список відкликаних сертифікатів.**

*Список відкликаних сертифікатів оновлюється впродовж двох годин з моменту зміни статусу сертифіката (блокування, розблокування, скасування). Список відкликаних сертифікатів оновлює оператор сертифікації.*

Оновлений список публікується протягом двох годин після отримання заявки на скасування, блокування або поновлення сертифіката.

Доступ до інформаційного ресурсу не обмежується. Термін зберігання списку відкликаних сертифікатів – необмежений.

## 6. Порядок генерації ключів підписувачів

Відкритий та особистий ключі підписувача можуть бути згенеровані за допомогою надійного засобу ЕЦП:

- самостійно, на особистому обладнанні;
- на робочій станції генерації ключів підписувачів в ЦСК або ВПР.

### 6.1 Генерація ключів на особистому обладнанні.

Для самостійної генерації відкритого та особистого ключів застосовуються надійні засоби ЕЦП, що надаються ЦСК. При цьому, генерація здійснюється з використанням технічних засобів заявника.

Згенерований особистий ключ підписувача захищається паролем та записується на носій ключової інформації. Відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе заявник.

Надійні засоби ЕЦП, що надаються заявнику, формують відкритий ключ підписувача у відповідному форматі.

Передача підписувачем сформованого відкритого ключа до ЦСК або ВПР здійснюється на носії інформації ним особисто або довіреною особою заявника.»

*Згідно ЗУ «Про електронний цифровий підпис» надійний засіб електронного цифрового підпису - це засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.*

*Для генерації відкритих та особистих ключів в якості надійного засобу ЕЦП АЦСК «Український сертифікаційний центр» на умовах договору з Клієнтом «Про надання послуг електронного цифрового підпису» надає Конфігурацію „Бест-Звіт Плюс”, яка є складовою частиною програмного комплексу «БЕСТ» та має експертний висновок Державної служби спеціального зв'язку та захисту інформації України від 14.12.2007 року №5/1-3435.*

*Носіями ключової інформації можуть бути дискети, USB-накопичувачі, CD тощо.*

*У випадку генерації ключів на особистому обладнанні підписувача, при отриманні відкритого ключа у відповідному форматі, адміністратор реєстрації перевіряє формат наданого відкритого ключа засобами програмного комплексу «БЕСТ», і у разі його невідповідності - відмовляє у формуванні сертифіката ключа. При цьому надані раніше документи повертаються заявнику з позначкою адміністратора реєстрації на заяві.*

*Під час обробки запиту на формування сертифіката ключа підписувача здійснюється перевірка належності особистого ключа підписувача відкритому ключу, який міститься у запиті. Перевірка здійснюється з використанням програмного комплексу «БЕСТ», автоматично, шляхом перевірки ЕЦП, накладеного на запит на формування сертифіката, з використанням відкритого ключа, що міститься у запиті. Тобто запит на формування сертифіката є самопідписаним. Формування сертифіката ключа підписувача можливе за умов успішної перевірки.*

*АЦСК «УСЦ» може видати сертифікати строком дії особистого ключа підписувача не більше ніж на 2 (два) роки. Початком перебігу строку дії особистого ключа підписувача вважається дата та час формування сертифіката, що містить відкритий ключ, відповідний до особистого.*

## 6.2 Генерація ключів на робочій станції ЦСК

Під час генерації ключів робоча станція від'єднується від комп'ютерної мережі шляхом зупинки мережевого з'єднання.

Ключі підписувача генеруються ним особисто на робочій станції адміністратора реєстрації, на якій встановлено надійний засіб ЕЦП програмний засіб в конфігурації „Бест-Звіт Плюс”, яка є складовою частиною програмного комплексу «БЕСТ» та має експертний висновок Державної служби спеціального зв'язку та захисту інформації України від 14.12.2007 року №5/1-3435 використовує бібліотеку функцій криптографічних перетворень (програмний вибір «NovaLib»), який має сертифікат відповідності за №424986 Серія ДС

Під час генерації ключів встановлюється шлях до з'ємного носія ключової інформації. Згенерований особистий ключ записується з пам'яті комп'ютера безпосередньо на з'ємний носій. Після запису знищується з пам'яті комп'ютера. Таким чином унеможливується виток інформації про особистий ключ під час генерації.

По закінченні процедури генерації особистий ключ підписувача захищається паролем і записується на носій ключової інформації, який залишається у підписувача, а відкритий ключ залишається на робочій станції адміністратора реєстрації.

Особисті ключі підписувачів не зберігаються в ЦСК.

Після генерації та запису особистого ключа підписувача на носій ключової інформації він автоматично знищується на станції генерації ключів надійним способом.

Генерація ключів довіреною особою здійснюється на робочій станції генерації ключів. По закінченні процедури генерації особистий ключ підписувача захищається паролем та записується на носій ключової інформації. Носій ключової інформації та пароль до особистого ключа вкладаються у непрозорий конверт, який запечатується, скріплюється печаткою ТОВ "УСЦ", підписами довіреної особи та адміністратора реєстрації.

Довірена особа робить запис на бланку про отримання конверта з носієм особистого ключа, паролем до особистого ключа та інструкції про порядок зміни паролю до особистого ключа підписувача. Документ із записом зберігається разом з документами заявника. Після передачі конверта з носієм ключової інформації довірений особі заявника, відповідальність за забезпечення конфіденційності та цілісності особистого ключа несе заявник.

У разі, якщо генерація ключів здійснювалась довіреною особою, заявник при отриманні від довіреної особи конверта з особистим ключем та паролем зобов'язаний виконати дії, наведені в інструкції, яка передається довірений особі, а саме:

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 CD-R), необхідно після зміни паролю зберегти особистий ключ на новому носії, а попередній носій особистого ключа знищити надійним способом, без можливості його відтворення;

при порушенні цілісності конверта, заявник (підписувач) невідкладно зобов'язаний звернутись до ЦСК із заявою про скасування сертифіката відповідного ключа.

## 7.1 Порядок створення сертифікатів відкритих ключів підписувачів, визнання сертифіката його власником.

Підписувач на один і той самий момент часу може мати і використовувати лише один особистий ключ, якому відповідає відкритий ключ із чинним сертифікатом ключа. Це обмеження не стосується електронної печатки.

Формат сертифіката відповідає вимогам Закону України "Про електронний цифровий підпис" та визначається відповідними технічними специфікаціями форматів представлення базових об'єктів національної системи ЕЦП.

Сертифікат створюється за заявкою на створення сертифікату. Заявка подається адміністратором реєстрації до ЦСК електронною поштою або на електронному носії інформації. Заявка підписана особистим ЕЦП адміністратора реєстрації. Опрацювання заявки здійснюється протягом робочого дня з моменту надходження заявки до ЦСК.

Формат сертифіката визначений в Технічних специфікаціях форматів представлення базових об'єктів, затверджених спільним наказом Держзв'язку та ДСТСЗІ СБ України № 99/166 від 11.11.2006.

ЦСК забезпечує унікальність розпізнавального імені підписувача, що міститься в сертифікаті. Для фізичної особи обов'язковими реквізитами розпізнавального імені є прізвище, ім'я, по батькові та ПІН (серія та номер паспорта), а для юридичної особи – назва юридичної особи відповідно до статуту (положення) та ідентифікаційний код за ЄДРПОУ.

Сформований сертифікат, за бажанням заявника, адміністратор реєстрації:

- записує на носій інформації та передає заявнику;
- надає сертифікат - документ у паперовій формі, який засвідчується печаткою ЦСК та власноручним підписом адміністратора реєстрації.

Сертифікат визначається прийнятим з моменту підпису власником паперового варіанту заявки на формування сертифікату, яка є копією електронного документу наданого для формування сертифікату.

На загальнодоступному ресурсі сертифікат публікується не пізніше, ніж за 15 хвилин після його створення.

Термін чинності сертифіката вказаний в сертифікаті.

*Формування сертифіката ключа підписувачу здійснюється на підставі даних, отриманих від заявника або його представника під час реєстрації.*

*Термін чинності сертифіката ключа, вказаний в сертифікаті, не може перевищувати двох років. Початком строку чинності сертифіката ключа вважається дата та час його формування.*

## 7.4 Порядок блокування сертифікатів ключів

Блокування сертифікату ключа - це тимчасове припинення чинності сертифікату ключа. *Процедуру блокування сертифіката виконує оператор сертифікації.*

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

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

Часом блокування сертифікату ключа вважається час зміни його статусу на інформаційному ресурсі ЦСК.

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

Згідно ЗУ «Про електронний цифровий підпис» ЦСК блокує сертифікат ключа:

- у разі подання заяви підписувача, Клієнта або його уповноваженого представника;
- за рішенням суду, що набрало законної сили;
- у разі отримання відомостей про компрометацію особистого ключа підписувача.

### 7.5 Порядок поновлення чинності сертифікатів ключів

Поновлення чинності сертифіката ключа можливе лише для заблокованих сертифікатів ключів, термін блокування яких не скінчився. Процедуру розблокування сертифіката виконує оператор сертифікації.

Для поновлення чинності сертифіката ключа, заявник подає до ЦСК або ВПР письмову заяву встановленого зразка.

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

Часом поновлення чинності сертифіката ключа вважається час зміни його статусу на інформаційному ресурсі ЦСК.

ЦСК поновлює блокований сертифікат ключа:

- у разі подання заяви Клієнтом або його уповноваженим представником;
- за рішенням суду, що набрало законної сили;
- у разі встановлення недостовірності відомостей про компрометацію особистого ключа.

Блокування, скасування, поновлення чинності сертифікату здійснюється протягом двох годин з моменту надходження заяви до ЦСК згідно наказу ТОВ «УСЦ» № 02/02 від 2008 р. «Про встановлення часу обробки заяв на зміну статусу сертифіката в ТОВ „УСЦ”».

### 7.6 Порядок скасування сертифікатів ключів

Скасування припиняє чинність сертифіката ключа. Скасовані сертифікати ключів поновленню не підлягають. Процедуру скасування сертифіката виконує оператор сертифікації.

#### 7.6.1 Скасування сертифіката за заявою у електронній формі

Електронна заява подається до ЦСК або ВПР за встановленою формою та засвідчується підписувачем своїм ЕЦП. Заяви приймаються на електронну адресу [status@ukrcc.com](mailto:status@ukrcc.com).

Розгляд та опрацювання заяви на скасування сертифіката ключа та інформування заявника про блокування здійснюється протягом двох годин з моменту надходження заяви до ЦСК.

#### 7.6.2 Скасування сертифіката за заявою у письмовій формі

Для скасування сертифіката ключа заявник зобов'язаний подати до ЦСК або ВПР письмову заяву встановленого зразка, засвідчену його особистим підписом. Якщо заявником є юридична особа, заява засвідчується підписом уповноваженого представника та печаткою юридичної особи.

Розгляд та опрацювання заяви на скасування сертифіката ключа та інформування заявника про блокування здійснюється протягом двох годин з моменту надходження заяви до ЦСК.

Часом скасування сертифікату вважається час, який вказаний для скасованого сертифіката в списку відкликаних сертифікатів.

**У випадку, якщо необхідне термінове скасування сертифіката ключа через об'єктивні обставини, з метою недопущення майнової шкоди, заявник (підписувач) має заблокувати сертифікат такого особистого ключа в усній формі та протягом терміну блокування подати заяву про скасування сертифіката ключа.»**

*ЦСК негайно скасовує сформований сертифікат ключа підписувача у випадках, передбачених ст.13 ЗУ «Про електронний цифровий підпис», а саме:*

- *набрання законної сили рішенням суду про скасування посиленого сертифіката ключа;*
- *смерті підписувача або оголошення його померлим за рішенням суду;*
- *визнання підписувача недієздатним за рішенням суду;*
- *припинення діяльності суб'єкта господарювання - заявника;*
- *розірвання підписувачем трудового договору з юридичною особою - заявником;*
- *надання заявником недостовірних даних;*
- *не поновлення заявником заблокованого сертифіката протягом 90 календарних днів;*
- *припинення (розірвання) договору приєднання "Про надання послуг електронного цифрового підпису";*
- *за заявою заявника або його уповноваженого представника.*

**Обставини, за яких сертифікат повинен бути скасований заявником.**

*Підписувач зобов'язаний звернутися до ЦСК щодо скасування сертифіката ключа у разі:*

*компрометації особистого ключа підписувача (факт або обґрунтована підозра того, що особистий ключ став відомий іншим особам, втрата можливості подальшого використання особистого ключа із будь-яких обставин, зокрема, втрата або пошкодження носія ключової інформації тощо);*

*зміни відомостей, зазначених у сертифікаті ключа: переведення на іншу посаду або звільнення з роботи підписувача (для сертифікатів, в яких зазначено посада його власника); зміна прізвища; виявлення помилок у реквізитах сертифіката ключа тощо.*

*Документи, що були підставою для скасування, блокування або поновлення сертифіката ключа, фіксуються та зберігаються у ЦСК.*

*Підписувач не має права використовувати особистий ключ для накладення ЕЦП, сертифікат ключа якого скасовано.*

### **8.1 Фізичне середовище**

**ЦСК розташований у приміщенні на третьому поверсі нежилого будинку, який знаходиться під охороною, за адресою: 04080, м. Київ, вул. Фрунзе, 102.**

**Приміщення ЦСК складається із чотирьох зон:**

- **серверна кімната, в якій розташована екранована шафа;**
- **спеціальне приміщення,**
- **приміщення архіву,**
- **адміністративне приміщення.**

**Обладнання програмно-технічного комплексу, що забезпечує формування сертифікатів, управління статусом сертифікатів та зберігання особистих ключів**

ЦСК, розміщується в екранованій шафі, яка знаходиться в серверній кімнаті та в спеціальному приміщенні.

Всі приміщення розміщуються в зоні основної будівлі на третьому поверсі та обладнані системою контролю доступу, охоронною та пожежною сигналізацією.

Серверна кімната забезпечує фізичний захист від несанкціонованого доступу до екранованої шафи, де встановлено відповідне обладнання. 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.

Приміщення ЦСК та програмно апаратний комплекс, який використовується для обслуговування сертифікатів, має експертний висновок та **ВІДПОВІДАЄ** вимогам нормативних документів систем технічного захисту інформації в Україні щодо захисту інформації.

Вхідні двері ЦСК стійкі до злому, обладнані трьома замками (двома механічними та одним магнітним).

Автоматизовані робочі місця адміністраторів та операторів ЦСК знаходяться у спеціальному приміщенні, доступ до якого обмежений. Робочі місця адміністраторів та операторів реєстрації знаходяться в контрольованій зоні.

Доступ до екранованої шафи ЦСК у режимі штатної роботи мають:

- керівник ЦСК;
- адміністратор безпеки;
- системний адміністратор;
- адміністратор БД.

Інші особи мають право доступу до екранованої шафи тільки в супроводі адміністратора безпеки або керівника ЦСК. Факти доступу до екранованої шафи фіксуються у журналі (з зазначенням ПІБ посадової особи, мети та часу доступу, списку відвідувачів) та засвідчуються підписом керівника ЦСК або адміністратора безпеки. Усі співробітники ЦСК, які мають право доступу до екранованої шафи, зобов'язані виконувати роботи тільки під час виконання своїх обов'язків.

Допуск у спеціальне приміщення у режимі штатної роботи ЦСК мають:

- керівник ЦСК;
- адміністратор безпеки;
- адміністратор сертифікації;
- оператор сертифікації;
- системний адміністратор;
- адміністратор БД;

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

В ЦСК відсутнє фізичне з'єднання внутрішньої локальної обчислювальної мережі із зовнішньої мережею (глобальною мережею), яка є доступною для користувачів. В ЦСК 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).

*Зона, що контролюється, обмежується: периметром офісного приміщення. Мінімальна відстань до місця можливого розташування рухомих засобів технічної розвідки складає 10м. Інопредставництва на відстані ближче ніж 200 м. відсутні.*

*Об'єкт призначений для оброблення інформації з вищою ступінню доступу «ДСК». Категорія обмеження доступу встановлена актом кате горювання від 24.03.2009р., згідно з яким об'єкт віднесено до четвертої категорії. Відповідно до Правил посиленої*

сертифікації, захист спеціального приміщення ЦСК «УСЦ» здійснюється відповідно до вимог НД ТЗІ для об'єктів ЕОТ третьої категорії, що підтверджується атестатом відповідності.

Серверна кімната забезпечує фізичний захист від несанкціонованого доступу до екранованої шафи, де встановлено відповідне обладнання. Екранована шафа забезпечує пасивний захист інформації від витоку каналами ПЕМВН, від порушення її цілісності внаслідок деструктивного впливу зовнішніх електромагнітних полів, яка забезпечує показник екранування у діапазоні від 0,1 до 1000 МГц, що підтверджено відповідними документами. Ефективність екранування екранованої шафи серверної ЦСК, розміщеної за у споруді №1, третій поверх, відповідає вимогам Правил посиленої сертифікації, розроблених на виконання постанови КМУ від 13 липня 2004 року за №903 згідно акту відповідності виданого НДЦ «Тезіс» НТУУ «КПІ».

### 8.3.2 Реєстраційний центр

До складу реєстраційного центру входить(ять) адміністратор(и) реєстрації.

**Функціональні обов'язки та відповідальність адміністратора реєстрації.**

Адміністратор реєстрації відповідає за:

- встановлення осіб, які звернулися до ЦСК для формування сертифіката;
- перевірку даних, обов'язкових для формування сертифіката, а також даних, які вносяться у сертифікат на вимогу підписувача;
- отримання від користувачів заявок на формування, скасування, блокування та поновлення сертифікатів ключів;
- надання консультацій підписувачам під час генерації ключів у разі отримання від них відповідного звернення та вживає заходи щодо забезпечення безпеки інформації під час генерації;
- забезпечення перевірки чинності звернень про блокування, поновлення та скасування сертифікатів;
- надає підписувачам консультації щодо умов та порядку надання послуг ЕЦП;
- інформує адміністратора безпеки про події, що впливають на безпеку функціонування акредитованого центру.

Адміністратор реєстрації виконує процедуру встановлення особи заявника (його довіреної особи), що проходить процедуру реєстрації.

Надані заявником (представником) документи розглядаються протягом однієї години з моменту їх надходження.

До розгляду не приймаються документи, які мають підчистки, дописки, закреслені слова, інші незастережні виправлення або написи олівцем, а також мають пошкодження, внаслідок чого їх текст неможливо прочитати.

За результатом розгляду наданих документів адміністратор реєстрації приймає рішення про відмову в реєстрації у разі:

- відсутності всіх необхідних для реєстрації документів;
- подання неналежно засвідчених копій документів;
- встановлення невідповідності даних, що визначені наданими документами, фактичним.

У випадку відмови у реєстрації, надані документи повертаються заявнику (представнику) з позначкою адміністратора реєстрації на заяві про підстави відмови.

При ухваленні позитивного рішення, після оформлення договірних документів та виконання заявником необхідних умов надання послуг ЕЦП (сплата послуг, подання додаткових документів, тощо) адміністратор реєстрації виконує дії по занесенню реєстраційної інформації до реєстру користувачів ЦСК.

Всі документи, що були надані заявникам під час реєстрації, беруться на облік шляхом формування справи підписувача, уведення необхідних ідентифікаційних даних

*підписувачів до БД ЦСК. Справа підписувача реєструється в журналі, який ведеться в паперовому або електронному вигляді.*

*Реєстрація заявника є підставою для генерації ключів заявника, створення запиту на сертифікацію та формування сертифіката ключа підписувача.*

*Всі дії адміністратор реєстрації виконує в межах затвердженої інструкції, яка опублікована на сайті [www.ukrcc.com](http://www.ukrcc.com).*

### **10.1 Порядок планової зміни ключів ЦСК**

**Планова зміна ключів ЦСК виконується не раніше, ніж через три роки та не пізніше, ніж через п'ять років після початку їх дії.**

**Процедура планової зміни ключів Центру здійснюється в такому порядку:**

**– посадові особи, призначені наказом директора ЦСК, в присутності адміністратора безпеки виконують генерацію нового особистого ключа ЦСК;**

*– генерація ключів виконується на комп'ютері відокремленому від локальної мережі на якому встановлена програмне забезпечення з «Програмно-апаратного комплексу “Український сертифікаційний центр” (експертний висновок ДСТСЗІ СБУ №18/2/1-4285 від 26.07.2006 р.), та записується на з'ємний носій. Після цього адміністратор сертифікації завантажує ключі до бази даних та формує запит на сертифікацію для надання до ЦЗО При завантаженні ключів призначаються два адміністратори сертифікації які надають право на використання особистого ключа посадовим особам ЦСК;*

*– службовими сертифікатами ЦСК є сертифікати сервісу TSP, сервісу OCSP, та оператора сертифікації. Сертифікати сервісів TSP та OCSP використовуються для надання послуг отримання позначки часу та отримання інформації про статус сертифіката в реальному часі відповідно. Сертифікати сервісу TSP, сервісу OCSP розташовані на загальнодоступному ресурсі. Сертифікат оператора сертифікації використовуються виключно для виконання посадових обов'язків та не розташовується на загальнодоступному ресурсі.;*

*– генерація ключів оператора виконується на робочому місці адміністратора сертифікації. Після створення особистого ключа оператора адміністрації посадова особа змінює пароль доступу по нього.*

**– адміністратор сертифікації ініціює процес засвідчення чинності відкритого ключа ЦСК в Центральному засвідчувальному органі шляхом передачі запиту на формування сертифіката;**

**– після отримання сертифіката від Центрального засвідчувального органу, новий сертифікат публікується на інформаційному ресурсі ЦСК.**

**Після публікації нового сертифіката на інформаційному ресурсі ЦСК (web-сторінці), старий особистий ключ знищується надійним способом.**

**Перевірка ЕЦП на документах, підписаних за допомогою старого особистого ключа, здійснюється шляхом застосування відповідного йому скасованого сертифіката ключа, який зберігається в інформаційному ресурсі ЦСК та в архіві Центрального засвідчувального органу.**