ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
"СВІЧ ГРУП"
49000, м. Дніпро, вул. Воскресенська, 30,
тел. (+380 56) 373-97-93

ЗАТВЕРДЖУЮ
Директор ТОВ «Свіч груп»

_____ Пашковська О.М.

«01» листопада 2020 р.

М.П.

Регламент роботи центру сертифікації ключів Товариства з обмеженою відповідальністю «Свіч груп»

37006207.001.Регламент ЦСК

ВИТЯГ

Аркушів 27

2020

ЗМІСТ

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

Регламент роботи центру сертифікації ключів товариства з обмеженою відповідальністю «Свіч груп» (далі – Регламент ЦСК) розроблено відповідно до вимог чинного законодавства України, яке регулює питання у сфері ЕП, а саме:

– Закон України “Про електронні документи та електронний документообіг”;

– Наказ Адміністрації Держспецзв'язку від 18.12.2012 № 739 «Про затвердження вимог до форматів криптографічних повідомлень».

– Інструкція про порядок забезпечення і використання ключів до засобів криптографічного захисту інформації, затверджена наказом Адміністрації Держспецзв'язку від 12.06.07 №114.

– ДСТУ 4145-2002 Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих;

– ДСТУ ГОСТ 28147-89 «Системи обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення»;

– ДСТУ 7564:2014 «Інформаційна технологія. Криптографічний захист інформації. Функція хешірування»;

– RSA/DSA з довжиною відкритого ключа 512-4096 біт

Регламент ЦСК визначає організаційні, технічні та інші умови діяльності центру сертифікації ключів товариства з обмеженою відповідальністю «Свіч груп» (далі – ЦСК) під час надання послуг електронного підпису (далі – ЕП).

Дія Регламенту ЦСК поширюється на:

– ЦСК, у тому числі відокремлені пункти реєстрації (за наявності);

– користувачів послуг ЕП, що надаються ЦСК: юридичних осіб публічного та приватного права всіх форм власності, фізичних осіб – суб’єктів підприємницької діяльності, фізичних осіб – громадян України, осіб без громадянства, іноземців.

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

ЦСК має право визначати обсяг положень Регламенту ЦСК або інших документів, з якими необхідно ознайомлювати користувачів.

1.1 Ідентифікаційні дані ЦСК

Повне найменування юридичної особи:
ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «СВІЧ ГРУП», «SWITCH GROUP» LIMITED;

Скорочені найменування юридичної особи:
ТОВ «СВІЧ ГРУП», «SWITCH GROUP» LTD;

Юридична та поштова адреса: 49000, Дніпропетровська обл., місто Дніпро, вулиця Воскресенська, будинок 30;

Телефон: (+380 56) 373-97-93;

Код ЄДРПОУ: 43773436;

Електронна адреса інформаційного ресурсу ЦСК: http://switchgroup.com.ua;
Адреса електронної пошти ЦСК: info@switchgroup.com.ua.

1.2 Визначення термінів, застосованих у Регламенті ЦСК

відокремлений пункт реєстрації – представництво (філія, підрозділ, дилер) ЦСК, яке здійснює реєстрацію підписувачів та забезпечує надання консультативних послуг клієнтам ЦСК;

заявник – фізична або юридична особа, яка звертається до ЦСК з метою формування сертифіката відкритого ключа;

клієнт (підписувач) – фізична або юридична особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний підпис під час створення електронного документа;

користувач послуг ЕП (користувач) – особа, яка перевіряє електронний підпис з використанням надійних засобів ЕП та даних про статус сертифікатів відкритих ключів;

надійний засіб електронного підпису – засіб електронного підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.
Підтвердження відповідності та проведення державної експертизи цих засобів здійснюється у порядку, визначеному законодавством;

реєстрація – встановлення особи заявника та перевірка інших наданих ним даних, що включаються у сертифікат;

сертифікація – формування сертифіката ключа, заснованого на перевірених при реєстрації даних, накладання на сертифікат підпису за допомогою особистого ключа ЦСК;

список відкликаних сертифікатів – перелік блокованих та скасованих сертифікатів, що формується та розповсюджується ЦСК;

подвійний контроль – спеціальна процедура доступу до даних, що передбачає участь двох осіб з відповідними повноваженнями для виконання завдання/процесу;

технологічний ключ уповноваженої посадової особи ЦСК – параметр криптографічного алгоритму формування електронного підпису, доступний

тільки конкретній посадовій особі ЦСК, призначений для автентифікації цієї особи при здійсненні внутрішніх технологічних операцій;

послуги ЕП – надання у користування засобів ЕП, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги.

Інші терміни вживаються у значеннях, визначених у Законі України "Про електронні документи та електронний документообіг".

У тексті Регламенту ЦСК застосовані також такі скорочення:

АС	–	автоматизована система
ЦСК	–	центр сертифікації ключів
БД	–	база даних
ВПР	–	відокремлений пункт реєстрації
ЕП	–	електронний підпис
КЗІ	–	криптографічний захист інформації
НСД	–	несанкціонований доступ
ПТК	–	програмно - технічний комплекс
СУБД	–	система управління базами даних
ТЗІ	–	технічний захист інформації.

1.3 Порядок внесення змін та доповнень до Регламенту ЦСК

Внесення змін та доповнень до цього Регламенту ЦСК здійснюється ЦСК у відповідності до чинного законодавства України. Зміни до Регламенту ЦСК затверджує директор.

Про внесення змін та доповнень до цього Регламенту ЦСК повідомляє заявників, підписувачів, користувачів та інших зацікавлених осіб шляхом розміщення зазначених змін та доповнень на електронному інформаційному ресурсі ЦСК.

Всі зміни та доповнення, внесені до Регламенту ЦСК, що не пов'язані зі зміною чинного законодавства України, набувають чинності через 10 (десять) календарних днів з моменту розміщення зазначених змін і доповнень на електронному інформаційному ресурсі ЦСК.

Всі зміни та доповнення, внесені Центром до Регламенту ЦСК у зв'язку зі зміною чинного законодавства України, набувають чинності одночасно зі вступом в силу відповідних норм нормативних актів.

2 ПЕРЕЛІК СУБ’ЄКТІВ, ЗАДІЯНИХ В ОБСЛУГОВУВАННІ І ВИКОРИСТАННІ СЕРТИФІКАТІВ КЛЮЧІВ ТА ЇХ ФУНКЦІЇ

2.1 Перелік суб’єктів

В обслуговуванні і використанні сертифікатів ЦСК задіяні наступні суб'єкти:

– ЦСК, в тому числі ВПР;

– підписувачі;

– користувачі.

2.2 Послуги, які надає ЦСК

ЦСК забезпечує надання повного переліку послуг ЕП, передбачених політикою сертифікації, зокрема:

1) реєстрація заявників;

2) надання у користування надійних засобів ЕП;

3) допомога при генерації відкритих та особистих ключів;

4) обслуговування сертифікатів ключів заявників, що включає:

– сертифікацію відкритих ключів заявників;

– розповсюдження та зберігання сертифікатів ключів;

– управління статусом сертифікатів ключів та розповсюдження інформації про статус сертифікатів ключів;

5) надання послуги фіксування часу.

Окрім надання послуг ЕП, ЦСК надає консультаційні послуги за зверненням заявників (підписувачів, користувачів).

Надання вищезазначених послуг здійснюється ЦСК відповідно до цього Регламенту ЦСК та на підставі укладених письмових договорів або договорів приєднання, укладених шляхом прийняття заяви-приєднання.

2.3 Відокремлені пункти реєстрації

Для наближення послуг ЕП до місцезнаходження заявників та підписувачів, можуть створюватись відокремлені пункти реєстрації. Відокремлені пункти реєстрації є відособленими підрозділами без правового статусу юридичної особи, що реалізують функції ЦСК з реєстрації заявників та їх подальшого обслуговування на відповідній території (крім формування сертифікатів та інформації про статус сертифікатів). Відокремлені пункти реєстрації не є юридичними особами, вони наділяються майном юридичної особи, діють на підставі Положення про відокремлений пункт реєстрації юридичної особи та цього Регламенту ЦСК.

Безпосереднє управління відокремленими пунктами реєстрації здійснюється ЦСК.

До складу відокремлених пунктів реєстрації входять:

– адміністратор реєстрації (керівник відокремленого пункту реєстрації);

– оператор реєстрації (діловод).

Функції та завдання відокремлених пунктів реєстрації:

– ідентифікація та верифікація осіб, які звернулися до ЦСК з метою формування сертифіката ключа;

– перевірка даних, обов'язкових для формування сертифіката ключа, а також даних, які вносяться у сертифікат ключа на вимогу заявника;

– проведення процедур реєстрації заявників (підписувачів);

– отримання від заявників (підписувачів) заявок на формування, скасування, блокування та поновлення сертифікатів ключів;

– надання допомоги підписувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вживання заходів щодо забезпечення безпеки інформації під час генерації;

– перевірка законності звернень про блокування, поновлення та скасування сертифікатів ключів;

– надання заявникам, підписувачам, користувачам консультацій щодо умов та порядку надання послуг ЕП;

2.4 Підписувачі та користувачі

Використовувати послуги ЦСК мають право як підписувачі так і користувачі.

Підписувачі користуються усім переліком послуг ЦСК на підставі укладеного договору та Регламенту ЦСК.

Користувачі, які хоч і не знаходяться у договірних відносинах з ЦСК але можуть використовувати надійні засоби ЕП для перевірки підпису або статусу сертифікатів, а також мають право використовувати інші послуги ЦСК, що не потребують автентифікації.

3 СФЕРА ВИКОРИСТАННЯ СЕРТИФІКАТІВ КЛЮЧІВ

3.1 Перелік сфер, у яких дозволяється використання сертифікатів ключів

Сертифікати ключів, сформовані ЦСК, використовуються для підтвердження ЕП, який задовольняє вимогам щодо підпису, застосованого до даних в електронній формі, у такий же спосіб, як власноручні підписи задовольняють вимогам стосовно документу на папері.

ЦСК здійснює обслуговування сертифікатів ключів, сформованих для підприємств, установ та організацій всіх форм власності (окрім державної), фізичних осіб, незалежно від сфери використання сертифікатів ключів.

3.2 Обмеження щодо використання сертифікатів ключів

ЦСК не встановлює обмеження щодо використання сформованих ним сертифікатів ключів.

4 ПОРЯДОК РОЗПОВСЮДЖЕННЯ (ПУБЛІКАЦІЇ) ІНФОРМАЦІЇ ЦСК

4.1 Інформаційний ресурс ЦСК

Інформаційний ресурс ЦСК призначений для розміщення на ньому відкритої інформації, яка структурно поділяється на:

– довідкова інформація (режими роботи ЦСК, положення Регламенту ЦСК, нормативні документи, договори на надання послуг, форми заяв тощо);

– сертифікат ЦСК;

– сертифікати серверів ЦСК;

– сертифікати підписувачів ЦСК;

– списки відкликаних сертифікатів, що містять інформацію про статуси сертифікатів ЦСК та підписувачів. Електронна адреса (DNS-ім'я) електронного інформаційного ресурсу switchgroup.com.ua.

Технічною основою інформаційного ресурсу ЦСК є web-сервери, що входять до складу ПТК ЦСК.

Довідкова інформація розміщується на web-сервері у вигляді набору web-сторінок.

Сертифікат ЦСК, сертифікати серверів ЦСК та підписувачів, а також списки відкликаних сертифікатів розміщуються:

– у складі web-сторінок на web-сервері;

– у інформаційному дереві LDAP-каталога на LDAP-сервері;

Доступ до web-сервера здійснюється за DNS-ім'ям switchgroup.com.ua за протоколом HTTP.

Доступ до LDAP-сервера здійснюється за DNS-ім'ям switchgroup.com.ua за протоколом LDAP.

4.2 Порядок публікації сертифікатів підписувачів

Публікація сертифікатів підписувачів на інформаційний ресурс ЦСК здійснюється за згодою підписувача. Інформація щодо можливості публікації сертифікату підписувача вноситься до реєстраційних даних під час реєстрації підписувача.

Після формування сертифікату ЦСК за наявності згоди підписувача протягом 1 години сертифікат публікується на інформаційному ресурсі.

4.3 Порядок публікації списків відкликаних сертифікатів

Публікація списку відкликаних сертифікатів на інформаційному ресурсі ЦСК (на web-сервері) здійснюється одразу після його випуску.

ЦСК формує список відкликаних сертифікатів одного типу:

– повний список.

Повний список випускається 1 (один) раз на добу або може випускатись до визначеного часу видання наступного повного списку та містить дані про всі сертифікати, відкликані (скасовані, блоковані) до закінчення строку їх дії.

5 ПОРЯДОК ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

5.1 Організаційні вимоги щодо встановлення заявника під час реєстрації

5.1.1 Загальні положення

Перед формуванням вперше сертифікатів ключів юридичним особам) або фізичним особам (ЕП використовується як аналог власноручного підпису та/або печатки) ЦСК здійснює встановлення (автентифікацію) заявника (фізичної або юридичної особи).

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

Заявник (або уповноважений представник заявника) повинен ознайомитися із умовами обслуговування сертифікатів ключів, передбачених політикою сертифікації, а також Регламентом ЦСК, зокрема:

– зобов'язання та підстави відповідальності ЦСК стосовно обслуговування сертифікатів ключів;

– зобов'язання та підстави відповідальності заявника (підписувача) стосовно використання сертифіката ключа і зберігання особистого ключа;

– сфери використання підписувачем сертифіката ключа;

– порядок перевірки чинності сертифіката ключа;

– строки зберігання ЦСК даних про заявників (підписувачів), що були отримані ним під час реєстрації;

– відомості про засоби ЕП, що можуть використовуватися для формування та перевірки ЕП.

5.1.2 Встановлення юридичної особи

Встановлення (автентифікація) заявника – юридичної особи здійснюється за установчими документами юридичної особи або копіями таких документів. Крім цього, під час реєстрації встановлюється представник юридичної особи та його повноваження.

Адміністратор реєстрації ЦСК з метою здійснення ідентифікації заявника зобов'язаний отримувати відомості, що містяться про нього в Єдиному державному реєстрі (у тому числі установчі документи юридичних осіб), у вигляді безоплатного доступу через портал електронних сервісів. Адміністратор реєстрації ЦСК отримує установчі документи юридичної особи шляхом їх пошуку за кодом доступу, наданого/введеного представником юридичної особи. Адміністратор реєстрації ЦСК зберігає отримані з Єдиного державного реєстру відомості про суб'єкта господарювання протягом всього часу обслуговування та використання сертифікатів ключів та їх функцій.

Заявник зобов'язаний повідомляти адміністратора реєстрації ЦСК про внесення змін до відомостей про нього, які містяться в Єдиному державному реєстрі, у тому числі до установчих документів юридичних осіб.

Представники заявника мають подати адміністратору реєстрації ЦСК документи, що підтверджують їх повноваження.

Особа, яка діє від імені заявника подає документи під час реєстрації, має пред'явити паспорт або інший документ, що посвідчує особу. Представники суб'єктів господарювання мають також надати документи, що підтверджують їх повноваження.

На підставі зазначених вище документів уповноважений адміністратор реєстрації ЦСК здійснює ідентифікацію заявника та ідентифікацію його уповноваженої особи (представника).

Під час реєстрації уповноважена особа заявника надає такі документи:

– заповнена та підписана заява на реєстрацію для отримання сертифіката ключа встановленого зразка у двох примірниках;

– заповнена та підписана заява-приєднання до договору "Про надання послуг електронного підпису";

– засвідчена копія установчого документа (статуту/ засновницького договору/установчого акту/положення). Юридичні особи, установчі документи яких оприлюднені на порталі електронних сервісів, установчий документ у паперовій формі не подають. При цьому, Адміністратор реєстрації ЦСК засвідчує своїм підписом/електронним підписом роздруковані/скопійовані відомості з Єдиного державного реєстру юридичних осіб, фізичних осіб - підприємців та громадських формувань (далі - Єдиний державний реєстр) про суб'єкта господарювання (у тому числі установчі документи юридичних осіб), отримані у вигляді безоплатного доступу через портал електронних сервісів.

– виписки з Єдиного державного реєстру юридичних осіб та фізичних осіб - підприємців, засвідчена підписом керівника та печаткою юридичної особи Заявника (за наявністю);

- паспорт (або інший документ, що посвідчує особу) Уповноваженої особи (фізичної особи), відкритий ключ електронного підпису якого

сертифікується (власник паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій, надає скан-копію ID-паспорт Уповноваженої особи (фізичної особи) а також довідку про присвоєння ідентифікаційного коду ДРФО (Реєстраційний номер облікової картки платника податків).

Уповноважена особа заявника має також надати документи, що підтверджують її повноваження.

На підставі зазначених вище документів Адміністратор реєстрації ЦСК здійснює ідентифікацію і верифікацію уповноваженої особи заявника.

Копії та витяги, посвідчуються підписом директора та печаткою юридичної особи (за наявністю).

У Заяві на реєстрацію для отримання сертифіката відкритого ключа юридичної особи вказується наступне: ідентифікаційні дані юридичної особи (найменування, ПІБ директора, номер свідоцтва про державну реєстрацію, номер за ЄДРПОУ, банківські реквізити), поштова та електронна адреси, номер телефону для зв'язку, вказівки щодо дозволу публікації сертифіката ключа, тип носія ключа, парольна фраза для ідентифікації підписувача по телефону (надається як додаток до заяви у опечатаному конверті).

5.1.3 Встановлення фізичної особи

Встановлення фізичної особи здійснюється за паспортом (або іншим документом, який засвідчує особу відповідно до законодавства України). Встановлення фізичної особи – підприємця здійснюється на підставі Виписки з Єдиного державного реєстру та документа, що посвідчує особу (паспорт).

У разі, якщо під час реєстрації встановлюється підписувач – фізична особа як представник юридичної особи, заявником виступає юридична особа. Встановлення заявника – юридичної особи здійснюється відповідно до п.5.1.2 Регламенту ЦСК.

У Заяві на реєстрацію для отримання сертифіката відкритого ключа фізичної особи – представника юридичної особи вказується наступне:

Ідентифікаційні дані юридичної особи (найменування, ПІБ директора, номер свідоцтва про державну реєстрацію, номер за ЄДРПОУ, банківські реквізити), поштова та електронна адреси, номер телефону для зв'язку, список фізичних осіб – підписувачів від юридичної особи, їх посади та паспортні дані, вказівки щодо дозволу публікації сертифіката, умови генерації ключів, тип носія ключа, парольна фраза для ідентифікації підписувача (підписувачів) по телефону (надається як додаток до заяви у опечатаному конверті).

Заява на реєстрацію фізичної особи – представника юридичної особи подається до ЦСК від імені юридичної особи – заявника, разом із паспортом фізичної особи. Власник паспорта у вигляді картки, що містить безконтактний електронний носій, надає копію (обох сторін) ID-паспорта Уповноваженої особи (фізичної особи), засвідчені підписом фізичної особи,

та відомостями щодо належності підписувача до цієї юридичної особи (завірена директором або керівником кадрового підрозділу юридичної особи та печаткою юридичної особи (за наявністю) довіреність.

Під час реєстрації заявник (фізична особа) надає такі документи:

для фізичних осіб – підприємців:

– заповнена та підписана заява на реєстрацію для отримання сертифіката ключа встановленого зразка у двох примірниках;

– заповнена та підписана заява приєднання до договору «Про надання послуг електронного підпису»;

– виписка з Єдиного державного реєстру, засвідчена підписом підприємця або підписом та печаткою посадової особи ЦСК;

– паспорт громадянина;

Копії та витяги, посвідчуються підписом підприємця та його печаткою (за наявністю).

Для фізичних осіб:

– заповнена та підписана заява на реєстрацію для отримання сертифіката ключа встановленого зразка у двох примірниках;

– заповнена та підписана заява-приєднання до договору «Про надання послуг електронного підпису»;

– паспорт фізичної особи;

– копія довідки про присвоєння ідентифікаційного коду ДРФО (Реєстраційний номер облікової картки платника податків).

Заявник може бути представлений довіреною особою, якщо немає можливості його особистої присутності у ЦСК. У цьому випадку заявник надає довіреність відповідного зразка. Встановлення представника здійснюється за паспортом або іншими документами відповідно до законодавства.

Довіреність на довірену особу заявника засвідчується:

– для юридичних осіб – підписом директора з прикладенням відбитку печатки юридичної особи (за наявністю);

– для фізичних осіб та фізичних осіб-підприємців – нотаріально.

Адміністратор реєстрації ЦСК 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 ЕП (попередня оплата, 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 бази даних ЦСК.

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

5.1.4 По завершенню процедури реєстрації, заявнику надаються:

– другий екземпляр заяви про реєстрацію для отримання сертифіката відкритого ключа з відмітками ЦСК;

– надійний засіб ЕП разом з інструкцією користувача в електронному вигляді.

5.1.5 Захист персональних даних підписувачів забезпечується шляхом вжиття:

– організаційних заходів щодо обліку та зберігання справ підписувачів, зокрема формування справи підписувачів та їх облік, призначення відповідальної особи за зберігання справ підписувачів, обмежений доступ обслуговуючого персоналу до приміщення (шаф), де зберігаються справи підписувачів;

– організаційно-технічних та технічних заходів реалізованих системою захисту інформації автоматизованої системи ЦСК, у тому числі: використанням надійних засобів ЕП, розмежування та контролю інформаційних потоків між внутрішньою локальною мережею ЦСК та

підсистемою відкритого доступу, використанням антивірусних засобів, міжмережевих екранів тощо.

5.1.6 Підтвердження володіння заявником (підписувачем) особистим ключем, відповідний якому відкритий ключ надається на сертифікацію.

Запит на сертифікацію в електронному вигляді містить відкритий ключ, що надається на сертифікацію та засвідчується ЕП за допомогою відповідного йому особистого ключа. Підтвердження володіння заявником (підписувачем) особистим ключем, відповідний якому відкритий ключ надається на сертифікацію здійснюється шляхом перевірки ЦСК (відокремленим пунктом реєстрації) ЕП запиту на формування сертифіката ключа.

6 УМОВИ, ПРОЦЕДУРИ ТА МЕХАНІЗМИ, ПОВ'ЯЗАНІ З ФОРМУВАННЯМ, БЛОКУВАННЯМ, СКАСУВАННЯМ ТА ВИКОРИСТАННЯМ СЕРТИФІКАТА КЛЮЧА

6.1 Порядок генерації ключів підписувачів

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

6.1.2 Генерація ключів підписувачам здійснюється надійними засобами ЕП, доступ до яких надається підписувачам через загальнодоступний інформаційний телекомунікаційний ресурс ЦСК, з використанням робочої станції генерації центру сертифікації ключів, або робочої станції клієнта.

6.1.3 При генерації ключів, надійний засіб ЕП формує запит на створення сертифікату у відповідному форматі (PKCS#10), який містить відкритий ключ підписувача і додаткову інформацію для випуску сертифікату. Зазначений запит для формування сертифікату передається до ПТК ЦСК захищеним каналом зв'язку. ЦСК, після перевірки коректності запиту, формує сертифікат підписувача та надає йому можливість одразу завантажити сертифікат у власний захищений носій.

6.1.4 Генерація ключів на робочій станції підписувача здійснюється після реєстрації підписувача. Для генерації ключів на робочій станції підписувача, використовується надійний засіб ЕП, який підписувач може завантажити на робочу станцію з інформаційного ресурсу ЦСК та встановити. Передача запиту на сертифікацію ключів здійснюється з використанням захищеного протоколу HTTPS. Згенерований особистий ключ підписувача записується на власний захищений носій інформації та захищається паролем. Засоби генерації ключів підписувача формують запит на створення сертифікату у відповідному форматі, який містить відкритий ключ підписувача і додаткову необхідну інформацію для випуску сертифікату Клієнта ЦСК.

6.1.5 Під час генерації ключів надійний засіб ЕП встановлений на робочій станції де здійснюється генерація ключів. Надійним засобом ЕП створюється пара: особистий ключ підписувача та відкритий ключ, який відповідає особистому. Інформація відкритого ключа з основними реквізитами підписувача засвідчується у встановленій ЦСК електронній формі запиту сертифікату.

6.1.6 Генерація нових ключів, подача запиту на новий сертифікат для підписувачів, які мають чинний сертифікат ключа може бути здійснена як на робочому місці підписувача, так і при особистій його присутності в пункті реєстрації ЦСК або ВПР на робочій станції ЦСК. При цьому запит обробляється в режимі реального часу (on-line або з затримкою 1-3 секунди) за допомогою ПТК ЦСК. Механізм аутентифікації підписувача, який має чинний сертифікат сформований ЦСК за допомогою засобів ПТК ЦСК здійснюється автоматично засобами ПТК ЦСК шляхом авторизації за допомогою логіну та паролю до власного облікового запису. ЦСК чи ВПР аутентифікує підписувача шляхом ознайомлення з документами, які посвідчують особу підписувача або за допомогою додаткових документів, які підписувач надає або пред'являє на вимогу ЦСК. Для формування нового сертифікату, підписувач, який має чинний сертифікат подає відповідну заяву та документи, перелік яких визначений Регламентом.

6.1.7 Строк дії особистого ключа підписувача становить до 1 (одного) року.

Строк дії ключів дорівнює строку чинності відповідного сертифіката.

Початком строку дії особистого ключа вважається дата та час формування сертифіката, що містить відкритий ключ відповідний до особистого.

6.2 Порядок подання запиту на сертифікацію

6.2.1 Для формування сертифікатів використовуються запити на формування сертифікатів підпису та шифрування, які створюються в процесі генерації особистого та відкритого ключа.

6.2.2 Якщо генерація особистих та відкритих ключів була проведена за межами ЦСК, запити на сертифікацію подаються адміністратору реєстрації відповідальною особою, яка пройшла процедуру ідентифікації та реєстрації.

6.3 Порядок формування сертифікатів ключів підписувачів

6.3.1 Після ідентифікації та реєстрації заявника відповідно до п.5 Регламенту та генерації ключів підписувача, адміністратор реєстрації виконує процедуру перевірки унікальності відкритих ключів підписувача в реєстрі сертифікатів ЦСК. Адміністратор сертифікації здійснює контроль за формуванням сертифікатів.

6.3.2 Строк обробки запиту на сертифікацію становить не більше чотирьох годин.

6.3.3 Сформовані сертифікати вносяться до реєстру сертифікатів ЦСК на інформаційному ресурсі ЦСК.

6.3.4 Після формування сертифіката ключа ЦСК адміністратор реєстрації виготовляє два примірника сертифіката у вигляді документа у паперовій формі, які засвідчуються печаткою (за наявністю) та підписом директора, а також власноручним підписом адміністратора реєстрації та адміністратора безпеки.

6.3.5 Сертифікат ключа підписувача в електронній формі записується на носій інформації заявника та у реєстр сертифікатів ЦСК.

6.3.6 Сертифікати підписувала, сформовані ЦСК чинні строком до 1 (одного) року.

6.3.7 Після отримання сертифікатів клієнт повинен перевірити достовірність відомостей, викладених у ньому. При виявлені недостовірних даних або помилок клієнт повинен повідомити ЦСК в порядку, визначеному для скасування сертифіката. Після скасування сертифіката та виправлення реєстраційних даних формується новий сертифікат.

6.4 Порядок повторного формування сертифіката

6.4.1 Повторне формування сертифіката ключа полягає у формуванні нового сертифіката ключа підписувачу, у разі завчасного (протягом дії договору) скасування чинного сертифіката, з підстав компрометації особистого ключа або зміни відомостей про заявника (підписувача), зазначених у сертифікаті ключа, який скасовано.

6.4.2 При повторному формуванні сертифіката ключа адміністратором реєстрації здійснюється перевірка дійсності даних, які надавалися заявником раніше під час реєстрації.

6.4.3 При виникненні необхідності зміни даних, зазначених у сертифікаті ключа, ЦСК здійснює повторне формування сертифіката ключа з перевидачею ключової пари.

6.5 Надання сформованого сертифіката ключа підписувачу та визнання сертифіката ключа його власником

6.5.1 У разі якщо запит на сертифікацію направлений заявником по електронній пошті, сертифікат ключа надсилається на електронну адресу, що зазначається підписувачем під час реєстрації. При особистій присутності підписувача в ЦСК під час формування сертифіката, сертифікат ключа надається особисто підписувачу.

6.5.2 Після отримання сертифіката ключа підписувач повинен перевірити правильність відомостей, що в ньому містяться. При виявленні некоректних даних (помилки в реквізитах), підписувач повинен повідомити про зазначене ЦСК (та/або відокремлений пункт реєстрації) у порядку, встановленому для скасування сертифіката ключа. В такому випадку сертифікат ключа скасовується та формується новий сертифікат ключа.

6.5.3 У разі, якщо протягом трьох робочих днів підписувач не звернувся до ЦСК щодо неприйняття сертифіката, сформований сертифікат вноситься до бази сертифікатів ЦСК та розміщується на інформаційному ресурсі ЦСК, якщо підписувач дав згоду на його публікацію.

6.5.4 Використання сертифікатів користувачем

Перед використанням сертифіката ключа користувач зобов'язаний:

– перевірити статус сертифіката ключа за актуальним списком відкликаних сертифікатів, або сервісом OCSP ЦСК;

– в разі використання списку відкликаних сертифікатів ключів, перевірити його автентичність і цілісність;

– використовувати сертифікат ключа ЦСК для перевірки справжності ЕП сертифікатів, які сформовані ЦСК;

– використовувати сертифікат ключа ЦЗО для перевірки справжності ЕП сертифіката ключа ЦСК.

Якщо одержання інформації про поточний стан сертифіката ключа є тимчасово неможливим, користувач повинен тимчасово відмовитись від використання сертифіката ключа.

6.6 Використання сертифіката та особистого ключа

6.6.1 Права та обов'язки підписувача (заявника)

Підписувач (заявник) зобов'язаний:

– ознайомитись та дотримуватись правил надання послуг ЕП;

– надавати повну та дійсну інформацію, необхідну для формування сертифіката підписувача;

– зберігати в таємниці особистий ключ та приймати всі можливі заходи для запобігання його втрати, розкриття, модифікації та несанкціонованого використання;

– не розголошувати та не повідомляти іншим особам пароль доступу до особистого ключа та ключову фразу для голосової автентифікації;

– використовувати особистий ключ виключно для мети, визначеної у сертифікаті, та додержуватись інших обмежень щодо використання сертифіката;

– використовувати надійні засоби ЕП для генерації особистих та відкритих ключів, формування та перевірки ЕП;

– негайно інформувати ЦСК про факти компрометації особистого ключа, компрометацію паролю захисту особистого ключа, виявлення неточностей або зміни даних у сертифікаті;

– не використовувати особистий ключ, відповідний до сертифіката, заява на блокування якого подана до ЦСК, протягом часу з моменту подання заяви і до моменту офіційного повідомлення про його поновлення;

– не використовувати особистий ключ, відповідний до сертифіката, заява на скасування якого подана до ЦСК, з моменту подання відповідної заяви;

– не використовувати особистий ключ, відповідний до сертифіката, що скасований або блокований.

Якщо заявник та підписувач є різними суб'єктами, заявник повинен зобов'язати підписувача виконувати вимоги Регламенту.

Підписувач (заявник) має право:

– своєчасно отримувати послуги ЕП;

– отримувати сертифікат ЦСК;

– отримувати списки скасованих сертифікатів, сформованих ЦСК;

– застосовувати сертифікат підписувача ЦСК для засвідчення (перевірки) ЕП електронних документів у відповідності до відомостей, які вказані у сертифікаті;

– застосовувати список скасованих сертифікатів, сформованих ЦСК, для засвідчення (перевірки) статусу власного сертифіката та сертифікатів інших підписувачів ЦСК;

– звертатися до ЦСК за засвідченням ЕП електронних документів;

– звертатися до ЦСК для скасування та блокування сертифіката протягом терміну дії відповідного особистого ключа;

– звертатися до ЦСК для поновлення заблокованого сертифіката протягом терміну дії відповідного особистого ключа та терміну, на який було блоковано сертифікат;

– вимагати від ЦСК виконання вимог конфіденційності;

– вимагати від ЦСК усунення порушень умов даного Регламенту ЦСК та договору про надання послуг ЕП в разі наявності цих порушень;

– оскаржити дії чи бездіяльність ЦСК у судовому порядку.

6.6.2 Права та обов'язки користувача

Користувач має право:

– цілодобового вільного доступу з використанням телекомунікаційних мереж загального користування до сертифікатів інших підписувачів, даних про статус сертифікатів, сертифіката ЦСК, нормативних документів з питань надання послуг ЕП;

– одержувати сертифікати ЦСК;

– одержувати списки відкликаних сертифікатів, сформовані ЦСК;

– ознайомлюватись з інформацією щодо діяльності ЦСК та надання послуг ЕП;

– використовувати надійні засоби ЕП;

– отримання консультацій з питань ЕП від ЦСК.

Користувач зобов'язаний:

– використовувати надійні засоби ЕП під час перевірки статусу сертифіката;

– здійснювати перевірку чинності сертифіката з використанням інформації про статус сертифіката;

– враховувати усі визначені у сертифікаті вимоги щодо його використання.

Користувач під час використання сертифіката несе відповідальність згідно чинного законодавства.

6.7 Процедура подачі запиту на сертифікацію для підписувачів, які мають чинний сертифікат ключа, сформований ЦСК

Процедура подачі запитів на сертифікацію для підписувачів, які мають чинний сертифікат ідентична процедурі подання запитів на сертифікацію для нового підписувача.

6.8 Підстави та порядок скасування, блокування та поновлення сертифікатів ключів

6.8.1 Підстави та порядок скасування сертифікатів ключів підписувачів

ЦСК негайно скасовує сформований сертифікат ключа підписувача у разі:

– набрання законної сили рішенням суду про скасування 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 30 календарних днів;

– припинення (розірвання) договору приєднання "Про надання послуг електронного підпису";

– за заявою заявника або його уповноваженого представника;

– закінчення строку чинності сертифіката ключа;

– компрометації особистого ключа.

6.8.2 Обставини, за яких сертифікат повинен бути скасований заявником

Підписувач (заявник – юридична особа) 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; втрата ключових носіїв з послідуючим їх знаходженням);

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

Під змінами обставин, на підставі яких було надано право володіння ЕП, слід розуміти зміни, які навіть при збереженні реквізитів підписувача змінюють його статус, що впливає на правомірність підпису. Зокрема, зміна положення про посаду підписувача, що призводить до того, що зазначені в сертифікаті ключа повноваження більше не належать підписувачу (в тому числі втрата права підпису звітності, керування банківським рахунком, проставляння печатки тощо).

Документи, що були підставами для скасування, блокування (поновлення) сертифіката ключа фіксуються та зберігаються в ЦСК.

Про факт зміни статусу сертифіката ключа ЦСК інформує підписувача електронною поштою, по телефону, або письмово.

6.8.3 Порядок скасування сертифікатів ключів

Скасування припиняє чинність сертифіката ключа. Скасовані сертифікати ключів поновленню не підлягають.

Для скасування сертифіката ключа заявник зобов'язаний подати до ЦСК письмову заяву встановленого зразка, засвідчену його особистим підписом. Якщо заявником є юридична особа, заява засвідчується підписом уповноваженого представника та печаткою юридичної особи (за наявністю). Опрацювання заяви на скасування сертифікату виконується протягом 1 (однієї) години робочого часу ЦСК (з 9.00 до 18.00) з моменту її отримання у письмової формі.

Часом скасування сертифіката ключа вважається час зміни його статусу в реєстрі сертифікатів ЦСК. Водночас з внесенням інформації про зміну статусу сертифікату до реєстру сертифікатів виконується розповсюдження

цієї інформації шляхом її внесення у список відкликаних сертифікатів та публікації списку відкликаних сертифікатів у загальнодоступному інформаційному ресурсі ЦСК.

У разі припинення діяльності заявника – юридичної особи, скасовуються всі чинні на момент скасування сертифікати ключів, в яких код ЄДРПОУ співпадає із кодом ЄДРПОУ юридичної особи, що припинила діяльність.

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

У випадку, якщо необхідне термінове скасування сертифіката ключа через об'єктивні обставини (наприклад, підтверджена компрометація особистого ключа), з метою недопущення спричинення майнової шкоди, заявник (підписувач) має право заблокувати сертифікат ключа такого особистого ключа в усній формі та протягом строку блокування подати відповідну заяву про скасування сертифіката ключа.

6.8.4 Порядок блокування сертифікатів ключів

6.8.4.1 Під блокуванням сертифіката ключа розуміється тимчасове припинення чинності сертифіката ключа.

Після блокування сертифіката ключа, заявник зобов'язаний протягом 30 календарних днів поновити строк чинності сертифіката ключа або подати заяву про його скасування. У випадку, якщо протягом зазначеного строку заявник не поновить чинність блокованого сертифіката ключа та не подасть заяви про його скасування, по закінченню вищезазначеного строку такий сертифікат ключа автоматично скасовується ЦСК.

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

Часом блокування сертифіката ключа вважається час зміни його статусу у реєстрі сертифікатів ЦСК.

6.8.4.2 Блокування сертифіката за заявою в усній формі

Заява в усній формі подається заявником (підписувачем) до ЦСК засобами телефонного зв'язку за номером, який опублікований ЦСК на власному інформаційному ресурсі, при цьому заявник повинен повідомити адміністратору реєстрації наступну інформацію:

– реєстраційний номер заявника;

– ідентифікаційні дані власника сертифіката;

– ключову фразу голосової автентифікації;

– реєстраційний номер сертифіката ключа.

Заява в усній формі приймається тільки у випадку позитивної автентифікації (збігу голосової фрази та ідентифікаційних даних підписувача з інформацією в реєстрі підписувачів).

Усна заява може бути подана цілодобово. Обробка усної заяви на блокування сертифіката та інформування власника сертифіката здійснюється протягом тридцяти хвилин з моменту подачі заяви. Усна заява повинна бути підтверджена письмовою заявою на протязі 7 (семи) робочих днів з часу прийняття усної заяви.

6.8.4.3 Блокування сертифіката за заявою у письмовій формі

Письмова заява подається до ЦСК або до ВПР за встановленою формою та засвідчується власноручним підписом заявника.

У разі якщо власником сертифіката є юридична особа, підпис уповноваженого представника юридичної особи засвідчується печаткою.

Подача письмової заяви на блокування сертифіката до ЦСК та її розгляд здійснюється протягом робочого дня.

Обробка такої заяви та інформування заявника про блокування повинні бути здійснені протягом одного робочого дня, що йде за робочим днем, протягом якого була подана заява.

6.8.4.4 Блокування сертифіката ключа за електронним запитом

Електронний запит на блокування сертифіката ключа передається до ПТК ЦСК у вигляді вкладення електронного поштового листа чи у вигляді http-запиту.

Електронний запит формується підписувачем за допомогою програмних засобів, які надаються ЦСК, а саме: з використанням інтерактивної http-форми «Залишити повідомлення», що розміщена на головній сторінці електронного інформаційного ресурсу: http://www.kfc.in.ua.

Електронний запит на блокування сертифіката ключа засвідчується ЕП відповідного сертифіката ключа підписувача.

У разі передачі запиту на блокування сертифіката ключа у вигляді http-запиту, обробка запиту та інформування підписувача про блокування здійснюються в режимі реального часу.

У разі передачі запиту на блокування сертифіката ключа засобами електронної пошти, обробка запиту та інформування підписувача про блокування повинні бути здійснені протягом 2 (двох) годин після отримання запиту ЦСК.

Заява у вигляді електронного запиту повинна бути підтверджена письмовою заявою на протязі 7 (семи) робочих днів з часу прийняття ЦСК електронного запиту.

6.8.5 Порядок поновлення чинності сертифікатів ключів

Поновлення чинності сертифіката ключа можливе лише для заблокованих сертифікатів ключів термін блокування яких не скінчився.

Для здійснення поновлення чинності сертифіката ключа, заявник подає до ЦСК або відокремленого пункту реєстрації, письмову заяву встановленого зразка.

Подача письмової заяви на поновлення чинності сертифіката ключа до ЦСК та її розгляд здійснюється тільки протягом робочого дня.

Обробка письмової заяви на поновлення чинності сертифіката ключа та інформування заявника про поновлення повинні бути здійснені протягом одного робочого дня, що йде за робочим днем, протягом якого була подана заява.

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

6.9 Закінчення строку чинності сертифіката ключа підписувача

Строк дії особистого та відкритого ключа дорівнює строку чинності відповідного сертифіката.

Після закінчення строку чинності сертифіката ключа, він вилучається з інформаційного ресурсу ЦСК та поміщається в архів.

ЦСК зберігає сертифікат та пов’язані з ним списки відкликаних сертифікатів безстроково. За запитом підписувачів, ЦСК надає доступ до необхідного сертифіката та пов’язаних з ним списків відкликаних сертифікатів з архівних записів ЦСК у строки, встановлені законодавством України для відповідей на звернення громадян.

6.10 Розповсюдження інформації про статус сертифікатів ключів

Для розповсюдження інформації про статус сертифіката ключа ЦСК використовується механізм списку відкликаних сертифікатів.

Публікація списку відкликаних сертифікатів здійснюється у відповідності з п.4.3 цього Регламенту ЦСК.

6.11 Дії у разі компрометації особистих ключів підписувачів ЦСК

Підписувач ЦСК самостійно приймає рішення щодо факту або загрози компрометації особистого ключа.

У випадку компрометації або загрози компрометації особистого ключа підписувач повинен виконати процедуру блокування або скасування сертифіката згідно положень цього Регламенту ЦСК.

Для поновлення сертифіката підписувачу необхідно виконати процедуру поновлення сертифіката у відповідності з умовами договору на надання послуг ЕП.

У разі скасування сертифіката підписувача внаслідок компрометації його секретного ключа здійснюється позапланова заміна сертифіката відкритого ключа у відповідності з умовами договору на надання послуг ЕП.

7 ПОРЯДОК НАДАННЯ ПОСЛУГ ФІКСУВАННЯ ЧАСУ

7.1 TSP система надає послугу фіксування часу по протоколу - Time Stamp Protocol (TSP).

7.2 TSP система надає послугу фіксування часу що відповідає умовам та вимогам до процедури засвідчення наявності електронного документа.

7.3 TSP система забезпечує виконання наступних функцій, пов’язаних із наданням послуг фіксуванням часу:

1) приймання та реєстрацію запитів на формування позначок часу;

2) формування позначок часу за допомогою особистого робочого ключа;

3) внесення сформованих позначок часу у реєстр позначок часу;

4) передача сформованої позначки часу;

5) зберігання та архівування позначок часу;

6) забезпечення синхронізації часу з всесвітнім координованим часом (UTC).

7.4 Використання позначок часу в електронному документообігу дозволяє створювати докази факту існування документа на визначений момент часу.

7.5 Позначка фіксування часу (time-stamp) — це є підписаний електронним підписом документ, яким сервер ЦСК підтверджує дійсність того, що у вказаний момент часу було надано значення геш –функції іншого конкретного документа, тобто є доказом, що деякі дані існували перед певним покажчиком часу. Значення геш-функції електронного документа забезпечує однозначний зв'язок позначки часу та документу.

7.6 Служба фіксування часу надає послуги в режимі транзакції, коли кожному запиту відповідає тільки одна мітка часу. Ініціатором транзакції виступає клієнт ЦСК з використанням наданого йому відповідного програмного забезпечення.

7.7 Запит позначки часу створюється засобами ПЗ клієнта за протоколом TSP з використанням об'єкту TSP-request.

7.8 При одержанні позначки часу, яка надходить від ЦСК протягом визначеного політикою ЦСК часу (за умовчанням - 1 секунда), клієнт (його ПЗ) повинен перевірити чинність:

– підпису позначки часу;

– відповідного сертифікату служби фіксування часу ЦСК;

7.9 Клієнт може застосувати позначку часу тільки в разі підтвердження її чинності.

7.10 Параметри запиту визначаються технічними характеристиками TSP-сервісів ЦСК. Служба фіксування часу має право відхиляти запити позначок часу, що не відповідають встановленим у ЦСК характеристикам.

7.11 Час, який використовується в позначці часу, встановлюється центром сертифікації ключів за київським часом на момент її формування та синхронізований із Всесвітнім координованим часом (UTC) з точністю до однієї секунди.

7.12 Центр сертифікації ключів отримує послугу з постачання передачі сигналів точного часу для формування та проведення перевірки позначки часу, надання якої забезпечується центральним засвідчувальним органом.

8 СЛУЖБА OCSP

8.1 Служба он-лайн статусу сертифікатів (OCSP Service-Online Certificate Service Protocol сервіс) призначена для перевірки стану чинності (валідності) сертифікату в режимі реального часу. Сервіс є складовою частиною ЦСК.

8.2 Звичайно стан чинності (валідності) сертифікату визначається за відсутністю запису про запрошуваний сертифікат у списках CRL, які формуються із заданою періодичністю. Служба OCSP дозволяє отримати інформацію про стан сертифікату безпосередньо у будь-який момент часу, навіть якщо запису про зміну стану сертифікату в CRL списках ще немає.

8.3 Запит стану сертифікатів виконується ПЗ клієнта за протоколом OCSP з використанням об'єкту OCSPRequest. Формування та додержання вимог протоколу та аналіз одержаного відгуку цілком покладається на клієнтське програмне забезпечення. ЦСК надає клієнту спеціальне ПЗ для формування запиту до служби OCSP.

8.4 Служба OCSP надає послуги в режимі трансакції, тобто кожному запиту відповідає один і лише один відгук, ініціатором транзакції виступає клієнт (клієнтське програмне забезпечення). Трансакція служби OCSP починається з підготовки запиту у визначеному форматі клієнтським програмним забезпеченням, яке надсилає його до служби OCSP.

8.5 Одержавши відповідь, клієнт повинен перевірити код відгуку та чинність електронного підпису. Якщо код відгуку не містить коду помилки та електронний підпис вірний, результат отриманого стану валідності сертифікатів вважається достовірним і може бути використаний в подальшій роботі.