ПОГОДЖЕНО

Перший заступник
Голови Держспецзв'язку

О.М. Чаузов

«16» 11 2016 року

ЗАТВЕРДЖУЮ

Міністр внутрішніх справ України

А.Б. Аваков

«21» листопада 2016 року

РЕГЛАМЕНТ РОБОТИ

АКРЕДИТОВАНОГО ЦЕНТРУ СЕРТИФІКАЦІЇ КЛЮЧІВ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ

На 57 аркушах

ПОГОДЖЕНО

Керівник центру сертифікації ключів МВС – начальник відділу сертифікації електронних ключів Департаменту інформаційних технологій МВС

О.В. Костюк

«14» листопада 2016 року

ПОГОДЖЕНО

Директор Департаменту інформаційних технологій МВС

В.А. Буржинський

«14» листопада 2016 року

Київ 2016

ЗМІСТ

ВСТУП

Терміни та визначення

У цьому Регламенті терміни та визначення вживаються у такому значенні:

автентифікація - процес, у тому числі електронний, який дає змогу підтвердити належність ідентифікаційних даних фізичній або юридичній особі;

автоматизована система - організаційно-технічна система акредитованого центру сертифікації ключів, що забезпечує обслуговування сертифікатів та об'єднує програмно-технічний комплекс, фізичне середовище, обслуговуючий персонал, а також інформацію, що обробляється в акредитованому центрі сертифікації ключів;

акредитація - процедура документального засвідчення компетентності центра сертифікації ключів здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів;

акредитований центр сертифікації ключів - центр сертифікації ключів, акредитований відповідно до Порядку акредитації центру сертифікації ключів, затвердженого постановою Кабінету Міністрів України від 13.07.2004 № 903;

блокування сертифіката ключа - тимчасове зупинення чинності сертифіката ключа;

відкритий ключ - параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;

електронний підпис - дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації Підписувача цих даних;

електронний цифровий підпис (ЕЦП) - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати Підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

засвідчення чинності відкритого ключа - процедура формування сертифіката відкритого ключа;

засіб електронного цифрового підпису - програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису;

захищений носій – надійний засіб електронного цифрового підпису, що призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на нього даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання;

Заявник - фізична або юридична особа, яка звертається до акредитованого центру сертифікації ключів з метою формування посиленого сертифіката (сертифікатів) ключів;

ідентифікаційні дані особи – унікальний набір даних, який дозволяє встановити тотожність фізичної або юридичної особи, або фізичної особи, яка представляє юридичну особу;

ідентифікація особи - встановлення тотожності фізичної або юридичної особи на підставі ідентифікаційних даних;

компрометація особистого ключа - будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа, у тому числі, втрата, крадіжка, несанкціоноване копіювання особистого ключа або паролю доступу до нього;

Користувач – фізична або юридична особа, яка перевіряє електронний цифровий підпис, накладений Підписувачем на електронний документ;

надійний засіб електронного цифрового підпису - засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації;

особистий ключ - параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки Підписувачу;

Підписувач - особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа;

повторне формування сертифіката - формування нового сертифіката акредитованим центром сертифікації ключів для Підписувача, який є власником чинного сертифіката, сформованого акредитованим центром сертифікації ключів;

посилений сертифікат відкритого ключа - сертифікат ключа, який відповідає вимогам Закону України «Про електронний цифровий підпис», виданий акредитованим центром сертифікації ключів (відповідно до Наказу Адміністрації Державної служби спеціального зв’язку та захисту інформації України № 739 від 18.12.2012 Центр може видавати сертифікат ЕЦП та сертифікат шифрування);

послуги електронного цифрового підпису - надання у користування засобів електронного цифрового підпису, 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, визначені Закону України «Про електронний цифровий підпис»;

представництва – відокремлений пункт реєстрації акредитованого центру сертифікації ключів, який здійснює реєстрацію Підписувачів та їх подальше обслуговування на відповідній території, територіальний орган, заклад, установа чи підприємство, що належать до сфери управління МВС, або центральний орган виконавчої влади, діяльність якого спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України, їх працівники, які в установленому порядку уповноважені МВС здійснювати в інтересах акредитованого центру сертифікації ключів процедури, визначені актами МВС та законодавством у сфері електронного цифрового підпису, а також треті особи, які в установленому порядку здійснюють представництво МВС та уповноважені здійснювати в інтересах акредитованого центру сертифікації ключів виключно процедуру встановлення, ідентифікації Заявників (зокрема фізичних та юридичних осіб при реєстрації Підписувачів, укладанні договорів про надання послуг електронного цифрового підпису) відповідно до вимог законодавства у сфері електронного цифрового підпису, із покладанням на них відповідальності за невиконання чи неналежне виконання своїх обов’язків згідно чинного законодавства;

програмно-технічний комплекс - апаратні, апаратно-програмні та програмні засоби акредитованого центру, що забезпечують виконання функцій, пов'язаних з наданням послуг електронного цифрового підпису;

реєстрація - встановлення Підписувача та перевірка наданих даних, що включаються у сертифікат;

розпізнавальне ім'я - сукупність реквізитів Підписувача, що забезпечують можливість однозначного визначення належності сертифіката цьому Підписувачу серед інших сертифікатів, сформованих у акредитованому центрі сертифікації ключів;

розповсюдження сертифіката ключа - надання сертифіката ключа Підписувачу - власнику особистого ключа або, у разі його згоди, іншим Користувачам;

розповсюдження інформації про статус сертифіката - надання вільного доступу до інформації про статус сертифіката у реальному часі у вигляді інформації про статус сертифіката, що оновлюється за визначеним періодом часу або у разі необхідності;

сертифікат відкритого ключа (далі - сертифікат ключа, сертифікат) - документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа Підписувачу. Сертифікати ключів можуть використовуватися для ідентифікації особи Підписувача;

сертифікація - формування сертифіката, заснованого на перевірених при реєстрації даних, накладання на сертифікат електронного цифрового підпису за допомогою особистого ключа акредитованого центру;

спеціальне приміщення - приміщення, яке відповідає вимогам, що наведені у додатку до пункту 4.1.1 Правил посиленої сертифікації, затверджених наказом ДСТСЗІ Служби безпеки України від 13.01.2005 №3 (у редакції наказу ДСТСЗІ Служби безпеки України від 10.05.2006 № 50) та зареєстровано в Міністерстві юстиції України від 27.01.2005 за № 104/10384;

список відкликаних сертифікатів - перелік блокованих та скасованих сертифікатів, що формується та розповсюджується акредитованим центром;

статус сертифіката - стан сертифіката ключа (чинний, блокований, скасований) на конкретний момент;

управління статусом сертифіката - зміна статусу сертифіката на підставі відповідних запитів та за умовами, визначеними Законом України «Про електронний цифровий підпис»;

центр сертифікації ключів - юридична особа незалежно від форми власності або фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги електронного цифрового підпису та засвідчила свій відкритий ключ у центральному засвідчувальному органі.

Інші терміни застосовуються у значеннях, наведених у Законі України від 22 травня 2003 року № 852-IV «Про електронний цифровий підпис» (зі змінами), Порядку акредитації центру сертифікації ключів, затвердженого постановою Кабінету Міністрів України від 13 липня 2004 року № 903, інших нормативно-правових актах з питань криптографічного та технічного захисту інформації, а також надання послуг ЕЦП з використанням паспорта громадянина України з імплантованим БЕН.

Статус Регламенту

Цей Регламент є нормативним документом, що визначає організаційні, технічні та інші умови діяльності Акредитованого центру сертифікації ключів Міністерства внутрішніх справ України (далі – Центр) під час надання послуг електронного цифрового підпису (далі – ЕЦП), у тому числі порядок та процедури обслуговування сертифікатів ключів Підписувачів.

Регламент розроблений відповідно до:

- Закону України від 22.05.2003 № 852- IV «Про електронний цифровий підпис» (зі змінами);

- Закону України від 22.05.2003 № 851 - IV «Про електронні документи та електронний документообіг» (зі змінами);

- Закону України від 15.05.2003 № 755 - IV «Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань» (у редакції від 26.11.2015 № 835 - VIII);

- Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу, затвердженого постановою Кабінету Міністрів України від 26.05.2004 № 680;

- Порядку акредитації центру сертифікації ключів, затвердженого постановою Кабінету Міністрів України від 13.06.2004 № 903;

- Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності, затвердженого постановою Кабінету Міністрів України від 28.10.2004 № 1452;

- Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України № 3 від 13.01.2005 (у редакції наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10.05.2006 № 50), зареєстрованим в Міністерстві юстиції України за № 568/12442 від 17.05.2006;

- інших нормативно-правових актів сфери надання послуг ЕЦП.

Норми цього Регламенту поширюються на:

- головний офіс Центру та його обслуговуючий персонал;
- представництва та їх обслуговуючий персонал;
- Заявників, Підписувачів та Користувачів послуг ЕЦП.

Вимоги Регламенту є обов’язковими до виконання обслуговуючим персоналом головного офісу Центру та представництв.

Умовою та підставою для укладання із Заявниками, Підписувачами та Користувачами послуг ЕЦП договору про надання послуг ЕЦП є визнання ними вимог Регламенту обов’язковими.

Будь-яка зацікавлена особа може ознайомитися з положеннями Регламенту на електронному інформаційному ресурсі Центру, в головному офісі Центра та офісах його представництв.

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим Регламентом, застосовуються правила міжнародного договору.

Внесення змін та доповнень до Регламенту

Внесення змін та доповнень до цього Регламенту здійснюється Центром відповідно до чинного законодавства.

Про внесення змін та доповнень до цього Регламенту, Центр повідомляє Заявників, Підписувачів, Користувачів послуг ЕЦП та інших зацікавлених осіб шляхом розміщення зазначених змін та доповнень на електронному інформаційному ресурсі Центру, а також шляхом розсилання повідомлень засобами електронної пошти.

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

Всі зміни та доповнення, внесені Центром до Регламенту у зв'язку зі зміною законодавства, набувають чинності одночасно зі вступом в силу відповідних нормативно-правових актів.

Договори та інші правочини, умови яких суперечать змінам чи доповненням до Регламенту, повинні бути переукладені протягом 10 (десяти) робочих днів з дня набрання чинності такими змінами.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Центр має такі ідентифікаційні дані.

Повні найменування юридичної особи: Міністерство внутрішніх справ України, the Ministry of Interior of Ukraine.

Скорочені найменування юридичної особи: МВС, the MIU.

Повні найменування Центру: Акредитований центр сертифікації ключів Міністерства внутрішніх справ України, Certification Authority of the Ministry of Interior of Ukraine.

Скорочені найменування Центру: АЦСК МВС України, CA of the MIU.

Юридична адреса: Україна, 01024, м. Київ, вул. Академіка Богомольця, 10.

Поштова адреса центрального офісу Центру: Україна, 01601, м. Київ, вул. Академіка Богомольця, 10.

Адреса розміщення центрального офісу Центру: Україна, 01024, м. Київ, вул. Академіка Богомольця, 10.

Телефон: +38 (044) 254-7719.

Код ЄДРПОУ: 00032684.

Електронна адреса інформаційного ресурсу Центру: ca.mvs.gov.ua

Адреса електронної пошти центрального офісу Центру: ca@mvs.gov.ua

2 ФУНКЦІЇ, ПРАВА ТА ОБОВ'ЯЗКИ ЦЕНТРУ, ЗАЯВНИКІВ, ПІДПИСУВАЧІВ ТА КОРИСТУВАЧІВ

2.1 Перелік суб'єктів, задіяних в обслуговуванні та використанні сертифікатів ключів

В обслуговуванні сертифікатів ключів та їх використанні задіяні такі суб'єкти:

- Центр у складі:
  - центральний офіс Центру;
  - представництва;
- Заявники;
- Підписувачі;
- Користувачі.

Центральний офіс Центру представлений окремим підрозділом або позаштатною структурою МВС, що здійснює надання послуг ЕЦП, забезпечує функціонування та розвиток Центру, виконання вимог законодавства до акредитованих центрів сертифікації ключів та у сфері захисту персональних даних.

Представництвами є:

- відокремлені пункти реєстрації, що представлені окремими підрозділами або позаштатними одиницями МВС та його територіальних органів, які підпорядковані центральному офісу Центру, та здійснюють надання послуг ЕЦП з реєстрації Підписувачів та їх подальше обслуговування на відповідній території;
- треті особи, які діють на підставі договору з МВС та уповноважені здійснювати в інтересах Центру виключно процедуру встановлення, ідентифікації Заявників та їх повноважень;
- територіальні органи, заклади, установи чи підприємства, що належать до сфери управління МВС, або центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України, їх працівники, які уповноважені МВС на підставі довіреності здійснювати в інтересах акредитованого центру сертифікації ключів відповідно до законодавства процедури, визначені актами МВС, зокрема, надання у користування засобів електронного цифрового підпису, допомоги при генерації відкритих та особистих ключів, встановлення, ідентифікацію Заявників (зокрема фізичних та юридичних осіб при реєстрації Підписувачів, укладанні договорів про надання послуг електронного цифрового підпису) відповідно до вимог законодавства у сфері електронного цифрового підпису, із покладанням на цих працівників відповідальності за невиконання чи неналежне виконання своїх обов'язків згідно з чинним законодавством.

Договори про надання послуг ЕЦП укладаються від імені МВС.

Заявниками можуть бути безпосередньо Підписувачі або уповноважені представники юридичних осіб – Підписувачів, які звертаються до Центру з метою формування сертифікатів для інших представників цієї юридичної особи.

Підписувачами та Користувачами можуть бути:

- юридичні особи та фізичні особи, які їх представляють (керівники органів управління, посадові особи, працівники, співробітники тощо);
- відокремлені підрозділи (філії) юридичних осіб та фізичні особи, які їх представляють (керівники органів управління, посадові особи, працівники, співробітники тощо);

- органи державної влади, органи місцевого самоврядування, установи та організації (далі – державні установи) та фізичні особи, які їх представляють (керівники органів управління, посадові особи, працівники, співробітники тощо);

- відокремлені підрозділи (філії) державних установ та фізичні особи, які їх представляють (керівники органів управління, посадові особи, працівники, співробітники тощо);

- фізичні особи – підприємці;

- самозайняті особи (приватні нотаріуси, адвокати, аудитори, арбітражні керуючі, оцінювачі та інші);

- наймані працівники фізичних осіб – підприємців та самозайнятих осіб (приватних нотаріусів, адвокатів, аудиторів, арбітражних керуючих, оцінювачів та інших);

- фізичні особи.

2.2 Функції, права та обов'язки Центру

2.2.1 Центр має право:

- отримувати та перевіряти інформацію, необхідну для реєстрації Підписувачів і формування посилених сертифікатів ключів, безпосередньо у юридичної або фізичної особи чи її представника;

- надавати послуги ЕЦП в обсягах, передбачених законодавством та на підставі укладених договорів, у тому числі:

  · надання у користування засобів ЕЦП;

  · надання допомоги при генерації відкритих та особистих ключів;

  · обслуговування сертифікатів ключів (реєстрація Підписувачів, формування, розповсюдження, скасування, зберігання, блокування та поновлення сертифікатів ключів);

  · надання інформації щодо чинних, скасованих і блокованих посилених сертифікатів ключів;

  · послуги фіксування часу;

  · консультації з питань ЕЦП;

  · інші послуги, які не суперечать вимогам законодавства;

- обслуговувати виключно посилені сертифікати ключів;

- вимагати від Заявників надавати повну та достовірну інформацію, необхідну для реєстрації Підписувачів та формування сертифікатів ключів, а також здійснювати перевірку наданої інформації;

- скасовувати, блокувати, поновлювати сертифікати ключів Підписувачів у порядку, визначеному цим Регламентом;

- вимагати від Підписувачів дотримуватись вимог цього Регламенту та умов договору про надання послуг ЕЦП;

- вимагати від Заявників зобов'язувати Підписувачів дотримуватись вимог цього Регламенту та умов договору про надання послуг ЕЦП;

- здійснювати переформування сертифіката Підписувачу із використанням попередньо засвідченого відкритого ключа Підписувача у разі, якщо відповідний йому особистий ключ не був скомпрометований, та з дотриманням вимог щодо недопущення

перевищення часу чинності особистого ключа та відповідного йому відкритого ключа більше двох років;

- припинити надання послуг ЕЦП Підписувачеві у разі порушення ним істотних умов договору про надання послуг ЕЦП та умов цього Регламенту;

- вимагати від Заявників та Підписувачів відшкодування в повному обсязі майнової та моральної шкоди у разі, якщо така шкода була завдана Центру з вини Заявників та Підписувачів;

- укладати договір із Заявником про надання послуг ЕЦП у формі електронного документа.

2.2.2 Центр зобов’язаний:

- забезпечувати захист інформації у своїх автоматизованих системах відповідно до законодавства;

- забезпечувати захист персональних даних, отриманих від Підписувача, відповідно до законодавства;

- використовувати для надання послуг ЕЦП надійні засоби ЕЦП;

- реєструвати та вести облік звернень фізичних та юридичних осіб, на підставі яких були сформовані сертифікати ключів;

- встановлювати відповідно до законодавства осіб, які звернулись до Центру з метою формування сертифіката ключа;

- перевіряти дані, обов'язкові для формування сертифіката ключа, і дані, які вносяться до нього на вимогу Підписувача;

- ознайомлювати Заявника із умовами обслуговування сертифікатів перед укладенням договору із Заявником щодо надання послуг ЕЦП, із наданням такої інформації через електронний інформаційний ресурс або в інший спосіб;

- формувати посилений сертифікат ключа згідно із законом та у форматі, визначеному законодавством;

- забезпечувати цілісність та автентичність сформованих сертифікатів;

- здійснювати формування, скасування, блокування та поновлення посилених сертифікатів ключів за участю або під контролем не менше ніж двох посадових осіб Центру відповідно до їх посадових обов'язків;

- під час реєстрації без розкриття особистого ключа Підписувача забезпечувати перевірку володіння Підписувачем особистим ключем, який відповідає відкритому ключу, наданому для формування сертифіката у разі, якщо особистий та відкритий ключі були згенеровані не Центром;

- забезпечувати унікальність розпізнавального імені Підписувача та реєстраційного номера сертифіката в межах Центру;

- перевіряти унікальність відкритого ключа Підписувача в реєстрі чинних, блокованих та скасованих сертифікатів;

- своєчасно попереджувати Підписувача та додавати в посилений сертифікат ключа Підписувача інформацію про обмеження використання ЕЦП, у тому числі ті, що встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку Центру;

- включати до посиленого сертифіката ключа електронну адресу електронного інформаційного ресурсу, де публікується список відкликаних сертифікатів Центру;

- включати до посиленого сертифіката ключа додаткові дані (належність до певної юридичної особи, посада тощо) на вимогу Підписувача або відповідно до вимог нормативно-правових актів, що встановлюють особливості застосування ЕЦП у відповідній сфері;

- забезпечувати доступність сертифіката Заявнику та/або Підписувачу, для якого цей сертифікат був сформований, після його формування;

- цілодобово забезпечувати доступність сертифіката для Користувачів у разі згоди на це Заявника, якщо для державних органів інше не передбачене правилами їх систем електронного документообігу;

- вести електронний перелік чинних, скасованих і блокованих сертифікатів ключів;

- забезпечувати зберігання сформованих посилених сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;

- забезпечувати резервування усіх сформованих сертифікатів;

- цілодобово приймати заяви про скасування, блокування та поновлення сертифікатів ключів;

- перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;

- своєчасно скасовувати, блокувати та поновлювати сертифікати ключів у випадках, передбачених законодавством;

- інформувати Підписувача, сертифікат якого був заблокований або скасований, про зміну статусу сертифіката;

- вносити зміни до списку відкликаних сертифікатів, доступних Користувачам, протягом не більше ніж дві години після отримання звернення Підписувача або його уповноваженого представника про скасування або блокування сертифіката;

- встановлювати за київським часом, синхронізованим з Всесвітнім координованим часом (UTC) з точністю до однієї секунди, час формування, скасування, блокування та поновлення сертифікатів ключів;

- забезпечувати протоколювання всіх подій, пов'язаних із формуванням, переформуванням, блокуванням, поновленням та скасуванням сертифікатів ключів, виданих Центром, із забезпеченням захисту протоколів від несанкціонованого доступу;

- при повторному формуванні сертифіката ключа здійснювати перевірку стосовно того, що інформація, яка надавалася раніше Заявником під час реєстрації, дійсна;

- забезпечувати цілодобовий доступ Користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів ключів через загальнодоступні телекомунікаційні канали;

- надавати Користувачам, які використовують сертифікати ключів, інформацію про необхідність здійснення перевірки чинності сертифіката ключа з використанням інформації про статус сертифіката ключа та врахування усіх визначених у сертифікаті вимог щодо його використання;

- включати до договорів про надання послуг ЕЦП умови надання доступу Користувачам до сертифікатів ключів Підписувачів (умови публікації сертифікатів) та обов'язки сторін, у тому числі, щодо обов'язковості використання надійних засобів ЕЦП;

- взяти на облік укладені договори із Заявниками, а також документи (посвідчені в установленому порядку копії документів), що використовуються під час реєстрації;

- надавати консультації з питань, пов'язаних з ЕЦП;

- здійснювати генерацію ключів Підписувачам за допомогою надійних засобів ЕЦП;

- у разі генерації ключів Підписувачам, вжити заходи конфіденційності під час генерації;

- забезпечити конфіденційність та цілісність особистого ключа у разі передачі ключа Підписувачу через Заявника;

- не допускати зберігання особистих ключів Підписувачів та ознайомлення з ними в Центрі;

- надавати Користувачам цілодобово через електронний інформаційний ресурс або в інший спосіб, що дає можливість ознайомлення, вільний доступ до інформації щодо умов, пов'язаних з використанням сертифікатів ключів, зокрема:

· положень політики сертифікації;

· обмежень при використанні сертифіката ключа;

· зобов'язань та підстав відповідальності Підписувачів стосовно використання сертифіката ключа, у тому числі щодо використання надійних засобів ЕЦП;

· інформації щодо порядку перевірки чинності сертифіката, у тому числі умов перевірки статусу сертифіката;

· строків зберігання Центром даних про Підписувачів, що були отримані ним під час реєстрації;

· порядку розв'язання спорів;

· законодавства в сфері ЕЦП;

· підстав відповідальності Центру;

- зобов'язати Заявника виконувати такі основні вимоги:

· надавати повну та дійсну інформацію під час реєстрації, необхідну для формування посиленого сертифіката ключа;

· використовувати особистий ключ виключно для ЕЦП, а також додержуватися інших вимог щодо його використання, визначених Центром у цьому Регламенті;

· зберігати особистий ключ у таємниці, не допускати використання особистого ключа іншими особами;

· використовувати надійні засоби ЕЦП для генерації особистих та відкритих ключів, формування та перевірки ЕЦП;

· негайно інформувати Центр про події, що трапилися до закінчення строку чинності сертифіката, а саме:втрату або компрометацію особистого ключа, втрату контролю щодо особистого ключа через компрометацію пароля, коду доступу до нього тощо, виявлену неточність або зміну даних, зазначених у посиленому сертифікаті ключа;

· не використовувати особистий ключ у разі його компрометації.

2.3 Функції, права та обов’язки Заявників, Підписувачів, Користувачів

2.3.1 Заявник та Підписувач мають право:

- своєчасно отримувати якісні послуги ЕЦП;

- одержувати сертифікати ключів Центру;

- одержувати списки відкликаних сертифікатів, сформованих Центром;

- застосовувати сертифікат Центру для перевірки справжності ЕЦП сертифікатів, сформованих Центром;

- застосовувати список відкликаних сертифікатів, сформованих Центром, та протокол інтерактивного визначення статусу сертифіката (OCSP) для перевірки статусу власного сертифіката та сертифікатів інших Підписувачів;

- генерувати відкриті та особисті ключі на своєму робочому місці з використанням надійного засобу ЕЦП, який надається Центром;

- ознайомлюватись з інформацією щодо діяльності Центру та надання послуг ЕЦП;

- подавати заяви, скарги, претензії;

- вимагати скасування, блокування або поновлення свого сертифіката ключа;

- вимагати від Центру усунення порушень умов даного Регламенту та договору про надання послуг ЕЦП;

- вимагати від Центру виконання вимог конфіденційності;

- оскаржувати дії чи бездіяльність Центру у судовому порядку.

2.3.2 Заявник та Підписувач зобов'язані:

- ознайомитись та дотримуватись правил надання послуг ЕЦП, вимог цього Регламенту та договору про надання послуг ЕЦП;

- надавати повну та дійсну інформацію під час реєстрації, необхідну для формування посиленого сертифіката ключа;

- використовувати особистий ключ відповідно до призначення ключа, зазначеному у сертифікаті відкритого ключа, а також додержуватися інших вимог щодо його використання, визначених Центром у цьому Регламенті;

- використовувати надійні засоби ЕЦП для генерації особистих та відкритих ключів, формування та перевірки ЕЦП;

- негайно інформувати Центр про події, що трапилися до закінчення строку чинності сертифіката, а саме: втрату або компрометацію особистого ключа, втрату контролю щодо особистого ключа через компрометацію пароля, коду доступу до нього тощо, виявлену неточність або зміну даних, зазначених у посиленому сертифікаті ключа;

- не використовувати особистий ключ у разі його компрометації.

- зберігати в таємниці особистий ключ та приймати всі можливі заходи для запобігання його втрати, розкриття, копіювання, перекручування та несанкціонованого використання;

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

- не використовувати особистий ключ, відповідний до сертифіката, заява на скасування чи блокування якого подана до Центру, протягом часу з моменту подання заяви і до моменту офіційного повідомлення про скасування сертифікату;

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

2.3.3 Користувач має право:

- одержувати сертифікати ключів Центру;

- одержувати сертифікати ключів Підписувачів у разі надання ними згоди на публікацію або використання сертифікатів;

- одержувати списки відкликаних сертифікатів, сформованих Центром;

- застосовувати сертифікат Центру для перевірки справжності ЕЦП сертифікатів, сформованих Центром;

- застосовувати список відкликаних сертифікатів, сформованих Центром, та протокол інтерактивного визначення статусу сертифіката (OCSP) для перевірки статусу сертифікатів Підписувачів;

- використовувати надійні засоби ЕЦП, надані Центром, для перевірки ЕЦП;

- ознайомлюватись з інформацією щодо діяльності Центру та надання послуг ЕЦП;

- отримувати послуги ЕЦП на правах Заявника та Підписувача;

- подавати заяви, скарги, претензії;

- вимагати від Центру усунення порушень умов даного Регламенту;

- оскаржувати дії чи бездіяльність Центру у судовому порядку.

2.3.4 Користувач зобов'язаний:

- перед перевіркою ЕЦП здійснювати перевірку чинності сертифіката ключа Підписувача на момент накладення ним ЕЦП, з використанням інформації про статус сертифіката, наданою Центром;

- враховувати усі визначені у сертифікатах ключів вимоги щодо сфери та обмежень їх використання.

3 СФЕРИ ВИКОРИСТАННЯ ТА ОБМЕЖЕННЯ ЩОДО ВИКОРИСТАННЯ СЕРТИФІКАТІВ КЛЮЧІВ

Центр має право встановлювати сфери використання та обмеження щодо використання сформованих ним сертифікатів ключів. Обмеження щодо використання сформованих Центром сертифікатів ключів застосовуються відповідно до положень законодавства України.

Для сертифікатів ключів, сформованих Підписувачам – представникам державних установ діють обмеження щодо використання ЕЦП, установлені в пункті 4 Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності, затвердженому постановою Кабінету Міністрів України від 28.10.2004 № 1452.

Інформація щодо обмеження сфери або сфер використання сертифіката доводиться до Заявника (Підписувача) та зазначається у сформованому Центром сертифікаті ключа.

Сфери, у яких дозволяється використання сертифікатів:

- у сфері надання послуг ЕЦП;
- для криптографічного захисту інформації шляхом її направленого шифрування відповідно до Наказу Адміністрації Державної служби спеціального зв’язку та захисту інформації України № 739 від 18.12.2012 (використовується сертифікат для шифрування);
- для ідентифікації користувачів в інформаційно-телекомунікаційних системах;
- в системах захисту від несанкціонованого доступу, у яких використовуються механізми автентифікації з використанням ЕЦП;
- для використання у якості електронної печатки.

Вищезазначений перелік не є вичерпним.

4 ПОРЯДОК РОЗПОВСЮДЖЕННЯ (ПУБЛІКАЦІЇ) ІНФОРМАЦІЇ ЦЕНТРОМ

4.1 Перелік інформації, що публікується Центром

На своєму електронному інформаційному ресурсі Центр публікує таку інформацію:

- загальні відомості про Центр;
- положення цього Регламенту;
- сертифікати ключів Центрального засвідчувального органу;
- сертифікати ключів Центру;
- сертифікати ключів серверів Центру (OCSP, TSP, CMP);
- сертифікати ключів Підписувачів, які надали згоду на їх публікацію;
- списки відкликаних сертифікатів, сформованих Центром;
- інформація щодо умов, пов'язаних з обслуговуванням та використанням сертифікатів ключів Підписувачів, зокрема:

· обмеження при використанні сертифіката ключа;

· зобов'язання та підстави відповідальності Підписувачів стосовно використання сертифіката ключа, у тому числі щодо використання надійних засобів ЕЦП;

· інформація щодо порядку перевірки чинності сертифіката ключа, у тому числі умов перевірки статусу сертифіката;

· строки зберігання Центром даних про Підписувачів, що були отримані ним під час реєстрації;

· порядок розв'язання спорів;

· вимоги законодавства в сфері електронного цифрового підпису;

· підстави відповідальності Центру;

· переліки та форми документів, які подаються до Центру для отримання послуг ЕЦП.

4.2 Час і порядок публікації сертифікатів та списків відкликаних сертифікатів

Сертифікати ключів Центру та серверів Центру публікуються одразу після їх формування або отримання від Центрального засвідчувального органу.

Сертифікати ключів Підписувачів, які надали згоду на їх публікацію, публікуються одразу після формування сертифікатів та виконання Підписувачем умов договору щодо обслуговування сертифікатів ключів.

Центр формує списки відкликаних сертифікатів у вигляді повного та часткового списків.

Повний список відкликаних сертифікатів формується та публікується 1 (один) раз на тиждень та містить інформацію про всі відкликані сертифікати ключів, які були сформовані Центром.

Частковий список відкликаних сертифікатів формується та публікується кожні 2 (дві) години та містить інформацію про всі відкликані сертифікати, статус яких був змінений в інтервалі між часом випуску останнього повного списку відкликаних сертифікатів та часом формування поточного часткового списку відкликаних сертифікатів.

5 ПОРЯДОК ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

5.1 Загальні положення

Ідентифікація та автентифікація Заявників та Підписувачів здійснюється Центром у випадках:

- звернення до Центру із заявою про реєстрацію;
- звернення до Центру із заявою на скасування сертифіката;
- звернення до Центру із заявою на блокування сертифіката;
- звернення до Центру із заявою на поновлення сертифіката;
- звернення до Центру про повторне формування сертифіката;
- здійснення Центром підтвердження володіння Підписувачем особистим ключем, відповідний якому відкритий ключ надається для сертифікації.

Ідентифікація здійснюється за ідентифікаційними даними, визначеними цим Регламентом.

Автентифікація здійснюється за механізмами, визначеними цим Регламентом, які передбачають:

- перевірку ідентифікаційних даних за документами або іншими відомостями, у тому числі в електронній формі, що підтверджують ідентифікаційні дані;
- голосову автентифікацію за ключовою фразою;
- електронну автентифікацію з використанням алгоритмів криптографічного захисту інформації.

Автентифікація за документами або іншими відомостями, у тому числі в електронній формі, що підтверджують ідентифікаційні дані осіб, які звернулись до Центру, здійснюється обслуговуючим персоналом Центру, на який покладено обов’язки адміністраторів реєстрації, чи представництва, у випадках подання:

- заяви про реєстрацію;
- заяви на скасування сертифіката;
- заяви на блокування сертифіката;
- заяви на поновлення сертифіката.

Голосова автентифікація за ключовою фразою здійснюється обслуговуючим персоналом Центру, на який покладено обов’язки адміністраторів реєстрації, у випадках подання заяви на блокування сертифіката в усній формі.

Електронна автентифікація з використанням алгоритмів криптографічного захисту інформації здійснюється засобами автоматизованої системи Центру у випадках:

- подання заяви на блокування сертифіката в електронній формі;
- здійснення Центром підтвердження володіння Підписувачем особистим ключем, відповідний якому відкритий ключ надається для сертифікації;
- подання заяви на повторне формування сертифіката в електронній формі.

5.2 Ідентифікація та автентифікація Заявників та Підписувачів під час подання заяв про реєстрацію

Реєстрація Підписувачів здійснюється Центром у випадках:

- особистого звернення Заявників із заявою про реєстрацію до Центру чи представництв (Заявники – Підписувачі);

- звернення представника відповідального підрозділу або спеціально визначеного працівника державної установи із заявою про реєстрацію працівників державної установи (Підписувачів), у тому числі за допомогою засобів телекомунікаційного зв'язку.

Форми заяв публікуються на електронному інформаційному ресурсі Центру.

У разі позитивної ідентифікації та автентифікації, адміністратор реєстрації Центру виконує дії із занесення ідентифікаційних даних Підписувача до реєстру Користувачів Центру.

Реєстрація є підставою для формування сертифіката ключа Підписувача.

Максимальний час між отриманням заяви про реєстрацію та формуванням сертифіката ключа Підписувача не повинен перевищувати двох годин.

У разі позитивної ідентифікації та автентифікації, всі документи, що були надані Заявниками під час реєстрації, окрім тих, що надавались для ознайомлення, залучаються до окремої справи Підписувача та передаються до архіву документів Центру.

Підстави відмови у наданні послуг ЕЦП:

- відсутність всіх документів, або інших відомостей, у тому числі в електронній формі, необхідних для ідентифікації та автентифікації Заявників та Підписувачів;

- подання документів, що мають підчистки, дописки, закреслені слова, інші незастережні та не засвідчені особистим підписом Підписувача виправлення, написи олівцем або мають пошкодження, внаслідок чого їх текст неможливо прочитати;

- подання неналежно засвідчених копій документів;

- встановлення невідповідності даних, що визначені наданими документами, або іншими відомостями, у тому числі в електронній формі, фактичним даним.

У разі негативної ідентифікації та автентифікації або відмови в розгляді письмових заяв про реєстрацію з причин, що наведено вище, всі документи, що були надані під час реєстрації, повертаються Заявникам із відміткою про причину відмови та повернення документів.

5.2.1 Ідентифікація та автентифікація юридичних осіб (окрім державних установ) та фізичних осіб – представників юридичних осіб, які особисто звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі)

Ідентифікація юридичних осіб здійснюється за такими ідентифікаційними даними:

- повне та скорочене (за наявності) найменування юридичної особи;

- місцезнаходження юридичної особи;

- ідентифікаційний код згідно з Єдиним державним реєстром юридичних осіб, фізичних осіб – підприємців та громадських формувань (далі – Єдиний державний реєстр);

- відомості про органи управління та їх склад.

Ідентифікація фізичних осіб – представників юридичних осіб (керівників органів управління, посадових осіб, працівників, співробітників тощо), які особисто звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі), здійснюється за такими ідентифікаційними даними:

- прізвище, ім'я, по батькові (за наявності);

- реєстраційний номер облікової картки платника податків (копія картки або сторінки паспорта громадянина України з відміткою про проставлення у паспорт реєстраційного номера облікової картки платника податків);

- серія, номер паспорта громадянина України (копії 1-2 сторінок паспорта (3-6 сторінок за наявності відміток) та копія сторінки паспорту з відміткою про відмову від прийняття реєстраційного номера облікової картки платника податків) - для фізичних осіб, які через свої релігійні переконання відмовились від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті;

- унікальний номер запису в Єдиному державному демографічному реєстрі - для володільців паспорта громадянина України у вигляді картки з імплантованим БЕН;

- займана посада по відношенню до юридичної особи, яку представляє фізична особа.

Автентифікація (встановлення) юридичних осіб та фізичних осіб – представників юридичних осіб (керівників органів управління, посадових осіб, працівників, співробітників тощо), які особисто звертаються до Центру для отримання послуг ЕЦП (Заявники – Підписувачі) здійснюється за документами або іншими відомостями, у тому числі в електронній формі, що підтверджують ідентифікаційні дані юридичних осіб та фізичних осіб – представників юридичних осіб.

Для автентифікації юридичних осіб використовуються :

- оригінали (для ознайомлення) та копії установчих документів юридичної особи, що підтверджують її ідентифікаційні дані, або інші відомості відповідно до Закону України від 15 травня 2003 року № 755 - IV «Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань».

Для автентифікації фізичних осіб використовуються:

- оригінали (для ознайомлення) та копії документів, що засвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані;

- копії документів, що засвідчують особу керівника юридичної особи та підтверджують її ідентифікаційні дані;

- копії документів, що підтверджують повноваження керівника юридичної особи;

- копії документів, що підтверджують повноваження (займану посаду) Підписувача - власника відкритого ключа.

Автентифікація (встановлення) юридичної особи та отримання ідентифікаційних даних щодо повноважень фізичної особи – представника юридичної особи з категорії осіб, які обираються (призначаються) до органу управління юридичної особи, уповноважених представляти юридичну особу в правовідносинах з третіми особами, або осіб, які мають право вчиняти дії від імені юридичної особи без довіреності, у тому числі підписувати договори, а також дані про наявність обмежень щодо представництва від імені юридичної особи, здійснюється з використанням інформації з Єдиного державного реєстру в електронному вигляді, що відображається на офіційному веб-сайті розпорядника Єдиного державного реєстру або веб-сайті технічного адміністратора Єдиного державного реєстру (далі – інформаційний ресурс Єдиного державного реєстру).

За наявності технічної можливості, додаткова автентифікація заявників здійснюється з використанням інформації з відповідних державних інформаційних систем (реєстрів, баз даних тощо) в електронному вигляді.

Копії документів засвідчуються відповідно до законодавства.

Перелік документів та роз’яснення щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Для укладання договорів про надання послуг ЕЦП Центр може отримувати від Заявників документи та інформацію, передбачені законодавством.

5.2.2 Ідентифікація та автентифікація відокремлених підрозділів (філій) юридичних осіб (окрім державних установ) та фізичних осіб – представників відокремлених підрозділів (філій) юридичних осіб, які особисто звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі)

Ідентифікація відокремлених підрозділів (філій) юридичних осіб здійснюється за такими ідентифікаційними даними:

- повне та скорочене (за наявності) найменування юридичної особи;
- повне та скорочене (за наявності) найменування відокремленого підрозділу (філії) юридичної особи;
- місцезнаходження юридичної особи;
- місцезнаходження відокремленого підрозділу (філії) юридичної особи;
- ідентифікаційний код згідно з Єдиним державним реєстром відокремленого підрозділу (філії) юридичної особи;
- відомості про органи управління та їх склад відокремленого підрозділу (філії) юридичної особи.

Ідентифікація фізичних осіб – представників відокремлених підрозділів (філій) юридичних осіб (керівників органів управління, посадових осіб, працівників, співробітників тощо), які особисто звертаються до Центру із заявою про реєстрацію ЕЦП (Заявники – Підписувачі), здійснюється за такими ідентифікаційними даними:

- прізвище, ім’я, по батькові (за наявності);
- реєстраційний номер облікової картки платника податків (копія картки або сторінки паспорта громадянина України з відміткою про проставлення у паспорт реєстраційного номера облікової картки платника податків);
- серія, номер паспорта громадянина України (копії 1-2 сторінок паспорта (3-6 сторінок за наявності відміток) та копія сторінки паспорту з відміткою про відмову від прийняття реєстраційного номера облікової картки платника податків) - для фізичних осіб, які через свої релігійні переконання відмовились від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті;
- унікальний номер запису в Єдиному державному демографічному реєстрі - для володільців паспорта громадянина України у вигляді картки з імплантованим БЕН;
- займана посада по відношенню до відокремленого підрозділу (філії) юридичної особи, який представляє фізична особа.

Автентифікація (встановлення) відокремлених підрозділів (філій) юридичних осіб та фізичних осіб – представників відокремлених підрозділів (філій) юридичних осіб (керівників органів управління, посадових осіб, працівників, співробітників тощо), які особисто звертаються до Центру для отримання послуг ЕЦП (Заявники – Підписувачі) здійснюється за документами або іншими відомостями, у тому числі в електронній формі, що підтверджують ідентифікаційні дані відокремлених підрозділів (філій) юридичних осіб та фізичних осіб – представників відокремлених підрозділів (філій) юридичних осіб.

Для автентифікації юридичних осіб використовуються :

- оригінали (для ознайомлення) та копії установчих документів відокремленого підрозділу (філії) юридичної особи, що підтверджують її ідентифікаційні дані, або інші відомості відповідно до Закону України від 15 травня 2003 року № 755 - IV «Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань».

Для автентифікації фізичних осіб використовуються:

- оригінали (для ознайомлення) та копії документів, що засвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані;

- копії документів, що засвідчують особу керівника відокремленого підрозділу (філії) юридичної особи та підтверджують її ідентифікаційні дані;

- копії документів, що підтверджують повноваження керівника відокремленого підрозділу (філії) юридичної особи;

- копії документів, що підтверджують повноваження (займану посаду) Підписувача - власника відкритого ключа.

Автентифікація (встановлення) відокремленого підрозділу (філії) юридичної особи здійснюється з використанням інформації з інформаційного ресурсу Єдиного державного реєстру, за наявності технічної можливості, додаткова автентифікація заявників здійснюється з використанням інформації з відповідних державних інформаційних систем (реєстрів, баз даних тощо) в електронному вигляді.

Копії документів засвідчуються відповідно до законодавства.

Перелік документів та роз'яснення щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Для укладання договорів про надання послуг ЕЦП Центр може отримувати від Заявників документи та інформацію, передбачені законодавством.

5.2.3 Ідентифікація та автентифікація державних установ та фізичних осіб – представників державних установ

Ідентифікація та автентифікація державних установ та фізичних осіб – представників державних установ, які звертаються до Центру за отриманням послуг ЕЦП, здійснюються із урахуванням Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності, затвердженого постановою Кабінету Міністрів України від 28.10.2004 № 1452 (далі – Порядок), відповідно до якого застосування електронного цифрового підпису в установі забезпечує підрозділ інформаційних технологій, а у разі відсутності такого - підрозділ, що виконує відповідні функції (далі - відповідальний підрозділ), або працівник, спеціально визначений наказом керівника цієї установи.

Ідентифікація державних установ здійснюється за такими ідентифікаційними даними:

- повне та скорочене (за наявності) найменування державної установи;

- місцезнаходження державної установи;

- ідентифікаційний код згідно з Єдиним державним реєстром;

- відомості про органи управління та їх склад.

Ідентифікація фізичних осіб – представників державних установ (керівників органів управління, посадових осіб, працівників, співробітників тощо) здійснюється за такими ідентифікаційними даними:

- прізвище, ім'я, по батькові (за наявності);

- реєстраційний номер облікової картки платника податків (копія картки або сторінки паспорта громадянина України з відміткою про проставлення у паспорт реєстраційного номера облікової картки платника податків);

- серія, номер паспорта громадянина України (копії 1-2 сторінок паспорта (3-6 сторінок за наявності відміток) та копія сторінки паспорту з відміткою про відмову від прийняття реєстраційного номера облікової картки платника податків) - для фізичних осіб, які через свої релігійні переконання відмовились від прийняття реєстраційного номера

облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті;

- унікальний номер запису в Єдиному державному демографічному реєстрі - для володільців паспорта громадянина України у вигляді картки з імплантованим БЕН;

- займана посада по відношенню до державної установи, яку представляє фізична особа.

Автентифікація (встановлення) державних установ та фізичних осіб – представників державних установ (керівників органів управління, посадових осіб, працівників, співробітників тощо) здійснюється за документами або іншими відомостями, у тому числі в електронній формі, що підтверджують ідентифікаційні дані державних установ та фізичних осіб – представників державних установ (керівників органів управління, посадових осіб, працівників, співробітників тощо).

Для автентифікації державних установ використовуються :

- оригінали або копії установчих документів державної установи (для ознайомлення), що підтверджують її ідентифікаційні дані, або інші відомості відповідно до Закону України від 15 травня 2003 року № 755 - IV «Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань».

Автентифікація (встановлення) державної установи та отримання ідентифікаційних даних щодо повноважень фізичної особи – представника державної установи з категорії осіб, які обираються (призначаються) до органу управління державної установи, уповноважених представляти державну установу в правовідносинах з третіми особами, або осіб, які мають право вчиняти дії від імені державної установи без довіреності, у тому числі підписувати договори, а також дані про наявність обмежень щодо представництва від імені державної установи, здійснюється з використанням інформації з інформаційного ресурсу Єдиного державного реєстру.

Для автентифікації фізичних осіб використовуються:

- оригінали (для ознайомлення) та копії документів, що засвідчують особу представника відповідального підрозділу або спеціально визначеного працівника державної установи, на якого покладено обов’язки забезпечення застосування електронного цифрового підпису в установі, та підтверджують його ідентифікаційні дані (надаються одноразово або у разі виникнення змін);

- копії документів, або інші відомості, у тому числі в електронній формі, що засвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані;

- копії документів або інші відомості, у тому числі в електронній формі, що підтверджують повноваження керівника державної установи;

- копії документів, що підтверджують повноваження представника відповідального підрозділу або спеціально визначеного працівника державної установи, на якого покладено обов’язки забезпечення застосування електронного цифрового підпису в установі (надаються одноразово або у разі виникнення змін);

- копії документів або інші відомості, у тому числі в електронній формі, що підтверджують повноваження (займану посаду) Підписувача - власника відкритого ключа.

Відповідно до Порядку, Центр за допомогою засобів телекомунікаційного зв’язку здійснює обмін інформацією, у тому числі ідентифікаційними даними для подальшої реєстрації Підписувачів, з представником відповідального підрозділу або спеціально визначеним працівником державної установи, відповідальним за застосування ЕЦП, із дотриманням вимог щодо забезпечення цілісності та конфіденційності інформації, із використанням надійних засобів ЕЦП та посилених сертифікатів відкритих ключів такого

працівника та представника державної установи з категорії осіб, які обираються (призначаються) до органу управління державної установи, уповноважених представляти державну установу в правовідносинах з третіми особами, або осіб, які мають право вчиняти дії від імені державної установи без довіреності, у тому числі підписувати договори.

Автентифікація за документами, що підтверджують ідентифікаційні дані Підписувачів, та підготовка ідентифікаційних даних для обміну із Центром здійснюється представником відповідального підрозділу або спеціально визначеним працівником державної установи, відповідальним за застосування ЕЦП.

Формат подання ідентифікаційних даних окремо узгоджується Центром та державною установою.

Ідентифікація та автентифікація представника відповідального підрозділу або спеціально визначеного працівника державної установи, відповідального за застосування ЕЦП, здійснюється виключно за його особистої присутності у представництві Центру.

За наявності технічної можливості, додаткова автентифікація державної установи, повноваження її керівника та посадових осіб здійснюється з використанням інформації з відповідних державних інформаційних систем (реєстрів, баз даних тощо) в електронному вигляді.

Копії документів засвідчуються відповідно до законодавства.

Перелік документів та роз’яснення щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Для укладання договорів про надання послуг ЕЦП Центр може отримувати від Заявників інші документи та інформацію, передбачені законодавством.

5.2.4 Ідентифікація та автентифікація відокремлених підрозділів (філій) державних установ та фізичних осіб – представників відокремлених підрозділів (філій) державних установ

Ідентифікація та автентифікація відокремлених підрозділів (філій) державних установ та фізичних осіб – представників відокремлених підрозділів (філій) державних установ, які звертаються до Центру за отриманням послуг ЕЦП, здійснюються із урахуванням Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності, затвердженого постановою Кабінету Міністрів України від 28.10.2004 № 1452, відповідно до якого застосування ЕЦП в установі (її відокремленому підрозділі, філії) забезпечує підрозділ інформаційних технологій, а у разі відсутності такого - підрозділ, що виконує відповідні функції (далі - відповідальний підрозділ), або працівник, спеціально визначений наказом керівника цієї установи (її відокремленого підрозділу, філії).

Ідентифікація відокремлених підрозділів (філій) державних установ здійснюється за такими ідентифікаційними даними:

- повне та скорочене (за наявності) найменування державної установи;
- повне та скорочене (за наявності) найменування відокремленого підрозділу (філії) державної установи;
- місцезнаходження державної установи;
- місцезнаходження відокремленого підрозділу (філії) державної установи;
- ідентифікаційний код згідно з Єдиним державним реєстром відокремленого підрозділу (філії) державної установи;
- відомості про органи управління та їх склад відокремленого підрозділу (філії) державної установи.

Ідентифікація фізичних осіб – представників відокремлених підрозділів (філій) державних установ (керівників органів управління, посадових осіб, працівників, співробітників тощо) здійснюється за такими ідентифікаційними даними:

- прізвище, ім’я, по батькові (за наявності);

- реєстраційний номер облікової картки платника податків (копія картки або сторінки паспорта громадянина України з відміткою про проставлення у паспорт реєстраційного номера облікової картки платника податків);

- серія, номер паспорта громадянина України (копії 1-2 сторінок паспорта (3-6 сторінок за наявності відміток) та копія сторінки паспорту з відміткою про відмову від прийняття реєстраційного номера облікової картки платника податків) - для фізичних осіб, які через свої релігійні переконання відмовились від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті;

- унікальний номер запису в Єдиному державному демографічному реєстрі - для володільців паспорта громадянина України у вигляді картки з імплантованим БЕН;

- займана посада по відношенню до відокремленого підрозділу (філії) державної установи, яку представляє фізична особа.

Автентифікація (встановлення) відокремлених підрозділів (філій) державних установ та фізичних осіб – представників відокремлених підрозділів (філій) державних установ (керівників органів управління, посадових осіб, працівників, співробітників тощо) здійснюється за документами або іншими відомостями, у тому числі в електронній формі, що підтверджують ідентифікаційні дані відокремлених підрозділів (філій) державних установ та фізичних осіб – представників відокремлених підрозділів (філій) державних установ (керівників органів управління, посадових осіб, працівників, співробітників тощо).

Для автентифікації відокремлених підрозділів (філій) державних установ використовуються :

- оригінали або копії установчих документів державної установи (для ознайомлення), що підтверджують її ідентифікаційні дані, або інші відомості відповідно до Закону України від 15 травня 2003 року № 755 - IV «Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань».

Автентифікація (встановлення) відокремленого підрозділу (філії) державної установи здійснюється з використанням інформації з інформаційного ресурсу Єдиного державного реєстру.

Для автентифікації фізичних осіб – представників відокремлених підрозділів (філій) державних установ використовуються:

- оригінали (для ознайомлення) та копії документів, що засвідчують особу представника відповідального підрозділу або спеціально визначеного працівника відокремленого підрозділу (філії) державної установи, на якого покладено обов’язки забезпечення застосування ЕЦП в установі, та підтверджують його ідентифікаційні дані (надаються одноразово або у разі виникнення змін);

- копії документів, або інші відомості, у тому числі в електронній формі, що засвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані;

- копії документів, або інші відомості, у тому числі в електронній формі, що підтверджують повноваження керівника відокремленого підрозділу (філії) державної установи;

- копії документів, що підтверджують повноваження представника відповідального підрозділу або спеціально визначеного працівника відокремленого підрозділу (філії)

державної установи, на якого покладено обов'язки забезпечення застосування ЕЦП в установі (надаються одноразово або у разі виникнення змін);

- копії документів, або інші відомості, у тому числі в електронній формі, що підтверджують повноваження (займану посаду) Підписувача - власника відкритого ключа.

Відповідно до Порядку, Центр за допомогою засобів телекомунікаційного зв'язку здійснює обмін інформацією, у тому числі ідентифікаційними даними для подальшої реєстрації Підписувачів, з представником відповідального підрозділу або спеціально визначеним працівником відокремленого підрозділу (філії) державної установи, відповідальним за застосування ЕЦП, із дотриманням вимог щодо забезпечення цілісності та конфіденційності інформації, із використанням надійних засобів ЕЦП та посилених сертифікатів відкритих ключів такого працівника та представника відокремленого підрозділу (філії) державної установи з категорії осіб, які обираються (призначаються) до органу управління відокремленого підрозділу (філії) державної установи, уповноважених представляти державну установу в правовідносинах з третіми особами.

Автентифікація за документами, що підтверджують ідентифікаційні дані Підписувачів, та підготовка ідентифікаційних даних для обміну із Центром здійснюється представником відповідального підрозділу або спеціально визначеним працівником відокремленого підрозділу (філії) державної установи, відповідальним за застосування ЕЦП.

Формат подання ідентифікаційних даних окремо узгоджується Центром та державною установою.

Ідентифікація та автентифікація представника відповідального підрозділу або спеціально визначеного працівника відокремленого підрозділу (філії) державної установи, відповідального за застосування ЕЦП, здійснюється виключно за його особистої присутності у представництві Центру.

За наявності технічної можливості, додаткова автентифікація відокремленого підрозділу (філії) державної установи, повноваження її керівника та посадових осіб здійснюється з використанням інформації з відповідних державних інформаційних систем (реєстрів, баз даних тощо) в електронному вигляді.

Копії документів засвідчуються відповідно до законодавства.

Перелік документів та роз'яснення щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Для укладання договорів про надання послуг ЕЦП Центр може отримувати від Заявників інші документи, передбачені законодавством.

5.2.5 Ідентифікація та автентифікація фізичних осіб – підприємців, які особисто звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі)

Ідентифікація фізичних осіб – підприємців здійснюється за такими ідентифікаційними даними:

- прізвище, ім'я, по батькові (за наявності);

- реєстраційний номер облікової картки платника податків (копія картки або сторінки паспорта громадянина України з відміткою про проставлення у паспорт реєстраційного номера облікової картки платника податків);

- серія, номер паспорта громадянина України (копії 1-2 сторінок паспорта (3-6 сторінок за наявності відміток) та копія сторінки паспорту з відміткою про відмову від прийняття реєстраційного номера облікової картки платника податків) - для фізичних осіб, які через свої релігійні переконання відмовились від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті;

- унікальний номер запису в Єдиному державному демографічному реєстрі - для володільців паспорта громадянина України у вигляді картки з імплантованим БЕН.

Автентифікація (встановлення) фізичних осіб – підприємців, які особисто звертаються до Центру для отримання послуг ЕЦП (Заявники – Підписувачі) здійснюється за документами, що підтверджують ідентифікаційні дані фізичних осіб – підприємців.

Для автентифікації фізичних осіб – підприємців використовуються :

- оригінали (для ознайомлення) та копії документів, що засвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані.

Копії документів засвідчуються відповідно до законодавства.

Перелік документів та роз'яснення щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Додаткова автентифікація фізичної особи – підприємця здійснюється з використанням інформації з Єдиного державного реєстру в електронному вигляді, що відображається на інформаційному ресурсі Єдиного державного реєстру.

Для укладання договорів про надання послуг ЕЦП Центр може отримувати від Заявників інші документи та інформацію, передбачені законодавством.

5.2.6 Ідентифікація та автентифікація самозайнятих осіб, які особисто звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі)

Ідентифікація самозайнятих осіб (приватний нотаріус, адвокат, оцінювач, аудитор, арбітражний керуючий тощо) здійснюється за такими ідентифікаційними даними:

- прізвище, ім'я, по батькові (за наявності);

- реєстраційний номер облікової картки платника податків (копія картки або сторінки паспорта громадянина України з відміткою про проставлення у паспорт реєстраційного номера облікової картки платника податків);

- серія, номер паспорта громадянина України (копії 1-2 сторінок паспорта (3-6 сторінок за наявності відміток) та копія сторінки паспорту з відміткою про відмову від прийняття реєстраційного номера облікової картки платника податків) - для фізичних осіб, які через свої релігійні переконання відмовились від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті;

- унікальний номер запису в Єдиному державному демографічному реєстрі - для володільців паспорта громадянина України у вигляді картки з імплантованим БЕН;

- адреса розташування робочого місця;

- номер документа, що підтверджує право самозайнятої особи на здійснення діяльності у певній сфері.

Автентифікація (встановлення) самозайнятих осіб, які особисто звертаються до Центру для отримання послуг ЕЦП (Заявники – Підписувачі) здійснюється за документами, що підтверджують ідентифікаційні дані самозайнятих осіб.

Для автентифікації самозайнятих осіб використовуються:

- оригінали (для ознайомлення) та копії документів, що засвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані.

Копії документів засвідчуються відповідно до законодавства.

Перелік документів та роз'яснення щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

За наявності технічної можливості, додаткова автентифікація самозайнятих осіб здійснюється з використанням інформації з відповідних державних інформаційних систем (реєстрів, баз даних тощо) в електронному вигляді.

Для укладання договорів про надання послуг ЕЦП Центр може отримувати від Заявників інші документи та інформацію, передбачені законодавством.

5.2.7 Ідентифікація та автентифікація фізичних осіб - найманих працівників фізичних осіб – підприємців та самозайнятих осіб, які звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі)

Ідентифікація та автентифікація фізичних осіб – підприємців (працедавців найманих працівників) здійснюється у порядку, встановленому пунктом 5.2.5 цього Регламенту, за винятком надання оригіналів документів, що засвідчують особу працедавців.

Ідентифікація та автентифікація самозайнятих осіб (працедавців найманих працівників) здійснюється у порядку, встановленому пунктом 5.2.6 цього Регламенту, за винятком надання оригіналів документів, що засвідчують особу працедавців.

Ідентифікація фізичних осіб - найманих працівників фізичних осіб – підприємців та самозайнятих осіб здійснюється за такими ідентифікаційними даними:

- прізвище, ім’я, по батькові (за наявності);
- реєстраційний номер облікової картки платника податків (копія картки або сторінки паспорта громадянина України з відміткою про проставлення у паспорт реєстраційного номера облікової картки платника податків);
- серія, номер паспорта громадянина України (копії 1-2 сторінок паспорта (3-6 сторінок за наявності відміток) та копія сторінки паспорту з відміткою про відмову від прийняття реєстраційного номера облікової картки платника податків) - для фізичних осіб, які через свої релігійні переконання відмовились від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті;
- унікальний номер запису в Єдиному державному демографічному реєстрі - для володільців паспорта громадянина України у вигляді картки з імплантованим БЕН;
- займана посада по відношенню до працедавця, яку представляє фізична особа – найманий працівник.

Автентифікація (встановлення) фізичних осіб - найманих працівників фізичних осіб – підприємців та самозайнятих осіб, які звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі) здійснюється за документами, що підтверджують їх ідентифікаційні дані.

Для автентифікації фізичних осіб - найманих працівників фізичних осіб – підприємців та самозайнятих осіб використовуються:

- оригінали (для ознайомлення) та копії документів, що підтверджують повноваження найманого працівника (Підписувача - власника відкритого ключа) та працедавця (трудовий договір (контракт) з відміткою про реєстрацію у центрі зайнятості);
- оригінали (для ознайомлення) та копії документів, що засвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані.

Копії документів засвідчуються відповідно до законодавства.

Перелік документів та роз’яснення щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

За наявності технічної можливості, додаткова автентифікація самозайнятих осіб здійснюється з використанням інформації з відповідних державних інформаційних систем

(реєстрів, баз даних тощо) в електронному вигляді.

Для укладання договорів про надання послуг ЕЦП Центр може отримувати від Заявників інші документи та інформацію, передбачені законодавством.

5.2.8 Ідентифікація та автентифікація фізичних осіб, які звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі)

Ідентифікація фізичних осіб здійснюється за такими ідентифікаційними даними:

- прізвище, ім’я, по батькові (за наявності);

- реєстраційні дані місця проживання (у разі вимоги Підписувача щодо внесення таких даних до сертифіката);

- реєстраційний номер облікової картки платника податків (копія картки або сторінки паспорта громадянина України з відміткою про проставлення у паспорт реєстраційного номера облікової картки платника податків);

- серія, номер паспорта громадянина України (копії 1-2 сторінок паспорта (3-6 сторінок за наявності відміток) та копія сторінки паспорту з відміткою про відмову від прийняття реєстраційного номера облікової картки платника податків) - для фізичних осіб, які через свої релігійні переконання відмовились від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку у паспорті;

- унікальний номер запису в Єдиному державному демографічному реєстрі - для володільців паспорта громадянина України у вигляді картки з імплантованим БЕН.

Автентифікація (встановлення) фізичних осіб, які особисто звертаються до Центру для отримання послуг ЕЦП (Заявники – Підписувачі) здійснюється за документами, що підтверджують ідентифікаційні дані фізичних осіб.

Для автентифікації фізичних осіб використовуються :

- оригінали (для ознайомлення) та копії документів, що засвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані.

Копії документів засвідчуються відповідно до законодавства.

Перелік документів та роз’яснення щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Для укладання договорів про надання послуг ЕЦП Центр може отримувати від Заявників інші документи та інформацію, передбачені законодавством.

5.2.9 Ідентифікація та автентифікація фізичних осіб - нерезидентів, які звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі)

Ідентифікація фізичних осіб - нерезидентів здійснюється за такими ідентифікаційними даними:

- прізвище, ім’я, по батькові (за наявності);

- реєстраційні дані місця проживання (у разі вимоги Підписувача щодо внесення таких даних до сертифіката);

- реєстраційний номер облікової картки платника податків (за наявності);

- серія та номер посвідки на постійне (тимчасове) місце проживання, у разі її відсутності – серія та номер паспорта громадянина іншої країни (посвідчення біженця).

Автентифікація (встановлення) фізичних осіб - нерезидентів, які особисто звертаються до Центру для отримання послуг ЕЦП (Заявники – Підписувачі) здійснюється за документами, що підтверджують ідентифікаційні дані фізичних осіб - нерезидентів. Якщо текст у документах викладений іноземною мовою, то разом з копіями таких документів

надається переклад на українську мову, засвідчений нотаріально.

Для автентифікації фізичних осіб - нерезидентів використовуються :

- оригінали (для ознайомлення) та копії документів, що засвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані.

Копії документів засвідчуються відповідно до законодавства.

Перелік документів та роз'яснення щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Для укладання договорів про надання послуг ЕЦП Центр може отримувати від Заявників інші документи та інформацію, передбачені законодавством.

5.3 Ідентифікація та автентифікація Заявників під час подання заяв на скасування, блокування та поновлення сертифікатів

Ідентифікація та автентифікація Заявників під час подання заяв на скасування, блокування та поновлення сертифікатів здійснюється у порядку, встановленому пунктами 6.5-6.7 цього Регламенту.

5.4 Підтвердження володіння Підписувачем особистим ключем, відповідний якому відкритий ключ надається для сертифікації

Підтвердження володіння Підписувачем особистим ключем, відповідний якому відкритий ключ надається для сертифікації, здійснюється шляхом електронної автентифікації з використанням алгоритмів криптографічного захисту інформації, реалізованих засобами автоматизованої системи Центру.

Механізм підтвердження володіння Підписувачем особистим ключем являє собою перевірку ЕЦП, накладеного на запит на формування сертифіката (запит на сертифікацію) особистим ключем Підписувача, за допомогою відкритого ключа, що міститься у запиті.

Підтвердження володіння Підписувачем особистим ключем здійснюється без розкриття особистого ключа.

Умови подання запиту на сертифікацію встановлено пунктом 6.1 цього Регламенту.

5.5 Ідентифікація та автентифікація Підписувачів при повторному формуванні сертифіката

Ідентифікація та автентифікація Підписувачів при повторному формуванні сертифіката здійснюється Центром у випадках:

- подання до Центру електронної заяви на повторне формування сертифіката після генерації нового особистого ключа;

- подання до Центру письмової заяви на повторне формування сертифіката при зміні даних про Підписувача, без генерації нового особистого ключа.

5.5.1 Ідентифікація та автентифікація Підписувачів у випадку подання до Центру електронної заяви на повторне формування сертифіката після генерації нового особистого ключа

Ідентифікація та автентифікація Підписувачів, у випадку подання до Центру електронної заяви на повторне формування сертифіката, після генерації нового особистого ключа, здійснюється з використанням алгоритмів криптографічного захисту інформації засобами автоматизованої системи Центру.

Заява на повторне формування сертифіката в електронному вигляді формується Підписувачем після генерації нового особистого ключа за допомогою надійних засобів ЕЦП, які надаються Центром. Заява на повторне формування сертифіката в електронній формі передається до автоматизованої системи Центру у вигляді вкладення електронного листа або у вигляді HTTP-запиту. При цьому, заява на повторне формування сертифіката в електронному вигляді засвідчується власним ЕЦП Підписувача, накладеним за допомогою попереднього особистого ключа.

Перевірка ідентифікаційних даних Підписувача, який звертається із заявою на повторне формування сертифіката в електронній формі, а також законності такого звернення, здійснюється шляхом автентифікації Підписувача та його повноважень шляхом перевірки ЕЦП на заяві та встановленням чинності на момент подання заяви сертифіката ключа, що містить ідентифікаційні дані особи.

У разі позитивної ідентифікації та автентифікації Підписувача у випадку подання ним заяви на повторне формування сертифіката в електронній формі у вигляді вкладення електронного листа, адміністратор реєстрації Центру виконує дії з формування нового сертифіката ключа Підписувача.

Максимальний час між отриманням заяви на повторне формування сертифіката в електронній формі у вигляді вкладення електронного листа та формуванням сертифіката ключа Підписувача не повинен перевищувати двох годин.

У разі передачі заяви на повторне формування сертифіката в електронній формі у вигляді HTTP-запиту, обробка запиту та інформування Підписувача про формування нового сертифіката здійснюються в режимі реального часу. Обробка запиту та інформування Підписувача про блокування сертифіката здійснюються в режимі реального часу.

5.5.2 Ідентифікація та автентифікація Підписувачів у випадку подання до Центру письмової заяви на повторне формування сертифіката при зміні даних про Підписувача без генерації нового особистого ключа

Ідентифікація та автентифікація Підписувачів у випадку подання до Центру письмової заяви на повторне формування сертифіката при зміні даних про Підписувача, без генерації нового особистого ключа, здійснюється відповідно до пункту 5.2 цього Регламенту.

У разі повторного формування сертифіката при зміні даних про Підписувача, зазначених у сертифікаті, окрім заяви на повторне формування сертифіката в письмовій формі, до Центру надаються копії документів, що підтверджують достовірність змін, які вносяться до сертифіката.

У разі позитивної ідентифікації та автентифікації Підписувача адміністратор реєстрації Центру скасовує діючий сертифікат та здійснює формування нового сертифіката Підписувачу із використанням попередньо засвідченого відкритого ключа Підписувача у разі, якщо відповідний йому особистий ключ не був скомпрометований, та з дотриманням вимог щодо недопущення перевищення строку чинності особистого ключа та відповідного йому відкритого ключа більше двох років.

6 УМОВИ, ПРОЦЕДУРИ ТА МЕХАНІЗМИ, ПОВ'ЯЗАНІ З ОБСЛУГОВУВАННЯМ ТА ВИКОРИСТАННЯМ СЕРТИФІКАТІВ КЛЮЧІВ

6.1 Подання запиту на сертифікацію та оброблення запиту

Запитом на сертифікацію є файл формату PKCS#10, що містить відкритий ключ Користувача і додаткову інформацію для формування сертифіката, який формується під час генерації особистого та відкритого ключів Підписувача надійними засобами ЕЦП, що надаються Центром.

Порядок надання надійних засобів ЕЦП та генерації особистих ключів Підписувачів встановлено пунктом 8.2 цього Регламенту.

Запит на сертифікацію подається до Центру в особі адміністратора реєстрації (віддаленого адміністратора реєстрації) разом із заявою на реєстрацію від осіб - Заявників, зазначених у Розділі 5 цього Регламенту, на носієві інформації.

Належність запиту на сертифікацію Заявникові підтверджується під час особистої передачі ним запиту адміністратору реєстрації (віддаленому адміністратору реєстрації).

Оброблення запиту на сертифікацію здійснюється Центром після ідентифікації та автентифікації особи, яка подає заяву, адміністратором реєстрації (віддаленим адміністратором реєстрації) та після підтвердження володіння Заявником відповідним особистим ключем відповідно до вимог цього Регламенту.

Оброблення запиту на сертифікацію здійснюється засобами автоматизованої системи Центру.

Під час обробки запиту на сертифікацію засобами автоматизованої системи Центру за участю адміністратора реєстрації (віддаленого адміністратора реєстрації) здійснюється перевірка унікальності відкритого ключа Підписувача в реєстрі чинних, блокованих та скасованих сертифікатів, унікальність розпізнавального імені Підписувача та унікальність реєстраційного номеру сертифіката ключа в межах Центру.

Використання особистого ключа Центру під час формування сертифікатів ключів Підписувачів забезпечується адміністратором сертифікації.

Засобами автоматизованої системи Центру забезпечується відповідність формату сертифіката ключа вимогам Закону України "Про електронний цифровий підпис" та Вимогам до формату посиленого сертифіката відкритого ключа, затвердженим наказом Міністерства юстиції, Адміністрації Держспецзв'язку від 20.08.2012 № 1236/5/453, зареєстрованого в Міністерстві юстиції 20.08.2012 за № 1398/21710.

Строк оброблення запиту на сертифікацію, поданого разом із заявою на реєстрацію, становить не більше двох годин.

6.2 Надання сформованого сертифіката ключа Підписувачу та визнання сертифіката його власником

Надання сформованого сертифіката ключа Підписувачу здійснюється в один із способів:

- шляхом надсилання файлу із сформованим сертифікатом ключа на адресу електронної пошти, вказану в заяві на реєстрацію;
- шляхом запису файлу із сформованим сертифікатом ключа на носій інформації, наданий Заявником;
- шляхом публікації сформованого сертифіката на електронному інформаційному ресурсі Центру.

Підписувач повинен перевірити свої ідентифікаційні дані, внесені до сертифікату ключа Центром. Центр повинен надавати відповідні консультації щодо проведення такої перевірки. Підписувач повинен використовувати особистий ключ тільки після проведення перевірки. Використання Підписувачем особистого ключа є фактом визнання ним сертифіката відповідного відкритого ключа.

У разі невідповідності ідентифікаційних даних, внесених Центром до сертифіката ключа та виявлених Підписувачем після отримання сформованого сертифіката ключа, власник сертифіката особисто або через уповноважену особу звертається до Центру для скасування сертифіката ключа та формування нового сертифіката у порядку, встановленому цим Регламентом.

У разі невідповідності ідентифікаційних даних, внесених Центром до сертифіката ключа та виявлених Центром до моменту надання сформованого сертифіката ключа Підписувачу, посадовою особою Центру здійснюється переформування сертифіката із використанням попередньо засвідченого відкритого ключа Підписувача та з дотриманням вимог щодо недопущення перевищення часу чинності особистого ключа та відповідного йому відкритого ключа більше двох років. Посадова особа, що здійснила переформування сертифіката, складає акт, в якому зазначається дата та час скасування сертифіката, ідентифікаційні дані Підписувача, що містяться в сертифікаті та невідповідні ідентифікаційні дані Підписувача, що зазначені у заяві про реєстрацію. Акт підписується посадовою особою Центру, що здійснила переформування сертифіката, та долучається до особової справи Підписувача.

6.3 Публікація сформованого сертифіката ключа Центром

Сформований Центром сертифікат ключа публікуються у порядку розповсюдження (публікації) інформації Центром, встановленим цим Регламентом (Розділ 4).

6.4 Використання сертифіката ключа та особистого ключа Підписувачем та сертифіката ключа Користувачем

Умови використання Підписувачем особистого ключа та власного сертифіката ключа, а також використання Користувачем сертифікатів ключів інших Підписувачів визначені у пункті 2.3 цього Регламенту.

6.5 Скасування сертифіката ключа

Центр негайно скасовує сформований ним сертифікат ключа у разі:

- закінчення строку чинності сертифіката ключа;
- подання заяви власника ключа (Підписувача) або його уповноваженого представника;
- припинення діяльності юридичної особи - власника ключа;
- смерті фізичної особи - власника ключа або оголошення його померлим за рішенням суду;
- визнання власника ключа недієздатним за рішенням суду;
- надання Центру власником ключа недостовірних даних;
- компрометації особистого ключа.

Скасування сертифіката ключа набирає чинності з моменту внесення його до списку відкликаних сертифікатів із зазначенням дати та часу здійснення цієї операції.

Скасований сертифікат ключа поновленню не підлягає.

Скасування сертифіката ключа за ініціативою Підписувача здійснюється за умови подання заяви на скасування сертифіката.

Заява на скасування сертифіката ключа подається до Центру Підписувачем або його уповноваженим представником за формою, яка публікується на електронному інформаційному ресурсі Центру.

Центр повинен встановити (ідентифікувати) особу, яка звертається із заявою на скасування сертифіката, а також перевірити законність такого звернення.

Перевірка ідентифікаційних даних особи, яка звертається із заявою на скасування сертифіката, а також законності такого звернення, здійснюється шляхом автентифікації особи та її повноважень за документами, що підтверджують ідентифікаційні дані особи.

Перелік документів та роз'яснення щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Максимальний час між отриманням заяви на скасування сертифіката та зміною його статусу, інформація про який доступна Користувачам, не повинен перевищувати двох годин.

Інформація про зміну статусу сертифіката ключа на «скасований» розповсюджується шляхом формування та публікації Центром списків відкликаних сертифікатів та за протоколом інтерактивного визначення статусу сертифіката (OCSP).

6.6 Блокування сертифіката ключа

Центр негайно блокує сформований ним сертифікат ключа у разі:

- подання заяви власника ключа (Підписувача) або його уповноваженого представника;
- за рішенням суду, що набрало законної сили;
- у разі компрометації особистого ключа.

Блокування сертифіката ключа набирає чинності з моменту внесення його до списку відкликаних сертифікатів із зазначенням дати та часу здійснення цієї операції.

Заява на блокування сертифіката ключа подається до Центру:

- письмово особисто Підписувачем або його уповноваженим представником за формою, яка публікується на електронному інформаційному ресурсі Центру;
- в електронній формі шляхом формування Підписувачем запиту на блокування сертифіката ключа із використанням особистого ключа та надійного засобу ЕЦП, наданого Центром;
- усно із проходженням процедури голосової автентифікації за ключовою фразою, обумовленою під час реєстрації Підписувача.

Центр повинен встановити (ідентифікувати) особу, яка звертається із заявою на блокування сертифіката, а також перевірити законність такого звернення.

Перевірка ідентифікаційних даних особи, яка звертається із письмовою заявою на блокування сертифіката, а також законності такого звернення, здійснюється шляхом автентифікації особи та її повноважень за документами, що підтверджують ідентифікаційні дані особи.

Перелік документів та роз'яснення щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Перевірка ідентифікаційних даних Підписувача, який звертається із заявою на блокування сертифіката в електронній формі, а також законності такого звернення, здійснюється шляхом автентифікації Підписувача та його повноважень шляхом перевірки ЕЦП на заяві та встановленням чинності на момент подання заяви сертифіката ключа, що містить ідентифікаційні дані особи.

Заява на блокування сертифіката в електронному вигляді формується Підписувачем за допомогою надійних засобів ЕЦП, які надаються Центром, та передається до автоматизованої системи Центру у вигляді вкладення електронного листа або у вигляді HTTP-запиту. При цьому, заява на блокування сертифіката в електронному вигляді засвідчується власним ЕЦП Підписувача.

Перевірка ідентифікаційних даних особи, яка звертається із усною заявою на блокування сертифіката, а також законності такого звернення, здійснюється шляхом автентифікації особи та її повноважень за ідентифікаційними даними особи, що містяться у сертифікаті та ключовою фразою, обумовленою під час реєстрації Підписувача.

За результатами обробки усної заяви на блокування сертифіката, посадова особа Центру, що прийняла заяву, складає акт, в якому зазначається дата та час подання заяви, ідентифікаційні дані Підписувача, що містяться в сертифікаті та ключова фраза, обумовлена під час реєстрації Підписувача. Акт підписується посадовою особою Центру, що прийняла заяву та долучається до особової справи Підписувача.

Максимальний час між отриманням заяви на блокування сертифіката та зміною його статусу, інформація про який доступна Користувачам, не повинен перевищувати двох годин.

У разі передачі заяви на блокування сертифіката в електронному вигляді у формі HTTP-запиту, обробка запиту та інформування Підписувача про блокування сертифіката здійснюються в режимі реального часу.

Інформація про зміну статусу сертифіката ключа на «блокований» розповсюджується шляхом формування та публікації Центром списків відкликаних сертифікатів та за протоколом інтерактивного визначення статусу сертифіката (OCSP).

Блокований сертифікат ключа може бути поновлений за умов, визначених у цьому Регламенті.

6.7 Поновлення сертифіката ключа

Центр поновлює заблокований сертифікат ключа у разі:

- подання заяви власника ключа (Підписувача) або його уповноваженого представника;
- за рішенням суду, що набрало законної сили;
- у разі встановлення недостовірності даних про компрометацію особистого ключа.

Поновлення сертифіката ключа за ініціативою Підписувача здійснюється за умови подання заяви на поновлення сертифіката.

Заява на поновлення сертифіката ключа подається до Центру Підписувачем або його уповноваженим представником за формою, яка публікується на електронному інформаційному ресурсі Центру.

Центр повинен встановити (ідентифікувати) особу, яка звертається із заявою на поновлення сертифіката, а також перевірити законність такого звернення.

Перевірка ідентифікаційних даних особи, яка звертається із заявою на поновлення сертифіката, а також законності такого звернення, здійснюється шляхом автентифікації особи та її повноважень за документами, що підтверджують ідентифікаційні дані особи.

Перелік документів та роз’яснення щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Максимальний час між отриманням заяви на поновлення сертифіката та зміною його статусу, інформація про який доступна Користувачам, не повинен перевищувати двох годин.

Інформація про зміну статусу сертифіката ключа на «чинний» розповсюджується шляхом формування та публікації Центром списків відкликаних сертифікатів та за протоколом інтерактивного визначення статусу сертифіката (OCSP).

6.8 Закінчення строку чинності сертифіката ключа Підписувача

Строк чинності сертифікатів ключів Підписувачів становить не більше двох років.

Дата та час початку та закінчення строку чинності сертифіката ключа Підписувача зазначається у сертифікаті.

Після перевершення дати та часу закінчення строку чинності сертифіката ключа Підписувача, сертифікат вважається нечинним, а електронний цифровий підпис, накладений із використанням відповідного особистого ключа Підписувача – недійсним.

8 УПРАВЛІННЯ КЛЮЧАМИ

8.2 Генерація ключів Підписувачів

Особистий та відкритий ключі Підписувача може бути згенерований:

– на робочому місці Підписувача;
– на робочій станції генерації ключів в офісах Центру.

Для генерації відкритого та особистого ключів на робочому місці Підписувача застосовуються надійні засоби ЕЦП, що надаються Центром.

Надійні засоби ЕЦП надаються Центром у вигляді апаратно-програмних засобів, окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків.

Надання Центром надійних засобів ЕЦП окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків, може здійснюватись шляхом передачі цих засобів на носіях інформації безпосередньо Підписувачеві або шляхом надання доступу через електронний інформаційний ресурс Центру.

Згенерований особистий ключ Підписувача захищається паролем та записується на носій ключової інформації НКІ. Відповідальність за забезпечення конфіденційності та цілісності власного особистого ключа несе сам Підписувач.

Надійні засоби ЕЦП під час генерації ключів формують запит на формування сертифіката (запит на сертифікацію) формату PKCS#10, що містить відкритий ключ Користувача і додаткову інформацію для формування сертифіката у Центрі.

Запит на сертифікацію подається до Центру в особі адміністратора реєстрації (віддаленого адміністратора реєстрації) разом із заявою на реєстрацію від осіб - Заявників, зазначених у Розділі 5 цього Регламенту, на носієві інформації або засобами електронної пошти під час попередньої реєстрації Заявників в електронній черзі Заявників.

Оброблення запитів на сертифікацію, поданих до Центру, здійснюється відповідно до пункту 6.1 цього Регламенту.

У разі генерації відкритого та особистого ключа Підписувача в офісі Центру, ключі генеруються ним особисто на робочій станції генерації ключів, що входить до складу автоматизованої системи Центру.

Для генерації відкритого та особистого ключів на робочій станції генерації ключів, що входить до складу автоматизованої системи Центру, на робочому місці Підписувача застосовуються надійні засоби ЕЦП у вигляді апаратно-програмних засобів та окремих програмних додатків.

Згенерований особистий ключ Підписувача захищається паролем та записується на носій ключової інформації. Відповідальність за забезпечення конфіденційності та цілісності власного особистого ключа несе сам Підписувач.

Запит на сертифікацію подається до Центру в особі адміністратора реєстрації (віддаленого адміністратора реєстрації) разом із заявою на реєстрацію від осіб - Заявників, зазначених у Розділі 5 цього Регламенту, на носієві інформації, окремому від носія ключової інформації.

Оброблення запитів на сертифікацію, поданих до Центру, здійснюється відповідно до пункту 6.1 цього Регламенту.

Особисті ключі Підписувачів (Користувачів) не зберігаються в Центрі.

Максимальний термін дії особистих та відкритих ключів Підписувача – 2 роки. Початок та завершення терміну дії особистих ключів зазначаються у відповідному сертифікаті відкритого ключа Підписувача.