

ПОГОДЖЕНО

Перший заступник
Голови Держспецзв'язку


О.М. Чаузов
« 27 » 09 2018 р.



ЗАТВЕРДЖУЮ

Міністр внутрішніх справ України


А. Б. Аваков
« 01 » 10 2018 р.



РЕГЛАМЕНТ РОБОТИ

АКРЕДИТОВАНОГО ЦЕНТРУ СЕРТИФІКАЦІЇ КЛЮЧІВ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ (НОВА РЕДАКЦІЯ)

На 57 аркушах

ПОГОДЖЕНО

Керівник акредитованого центру
сертифікації ключів МВС України –
начальник управління забезпечення
діяльності акредитованого центру
сертифікації ключів МВС України


О. В. Костюк
« 29 » серпня 2018 р.

ПОГОДЖЕНО

Директор Департаменту
інформатизації МВС України


І. П. Бондаренко
« 29 » серпня 2018 р.

ЗМІСТ

ВСТУП.....	4
Терміни та визначення	4
Статус Регламенту	6
Внесення змін та доповнень до Регламенту.....	7
1. ЗАГАЛЬНІ ПОЛОЖЕННЯ.....	9
2 ФУНКЦІЇ, ПРАВА ТА ОБОВ'ЯЗКИ ЦЕНТРУ, ЗАЯВНИКІВ, ПІДПISУВАЧІВ ТА КОРИСТУВАЧІВ	10
2.1 Перелік суб'єктів, задіяних в обслуговуванні та використанні сертифікатів ключів	10
2.2 Функції, права та обов'язки Центру	11
2.3 Функції, права та обов'язки Заявників, Підписувачів, Користувачів.....	14
2.3.1 Заявник та Підписувач мають право:.....	14
2.3.2 Заявник та Підписувач зобов'язані:	15
2.3.3 Користувач має право:.....	16
2.3.4 Користувач зобов'язаний:	16
3 СФЕРИ ВИКОРИСТАННЯ ТА ОБМЕЖЕННЯ ЩОДО ВИКОРИСТАННЯ СЕРТИФІКАТІВ КЛЮЧІВ	17
4 ПОРЯДОК РОЗПОВСЮДЖЕННЯ (ПУБЛІКАЦІЇ) ІНФОРМАЦІЇ ЦЕНТРОМ	18
4.1 Перелік інформації, що публікується Центром	18
4.2 Час і порядок публікації сертифікатів та списків відкликаних сертифікатів	18
5 ПОРЯДОК ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ	20
5.1 Загальні положення	20
5.2 Ідентифікація та автентифікація Заявників та Підписувачів під час подання заяв про реєстрацію	20
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).....	21
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)	23
5.2.3 Ідентифікація та автентифікація державних установ та фізичних осіб – представників державних установ.....	24
5.2.4 Ідентифікація та автентифікація відокремлених підрозділів (філій) державних установ та фізичних осіб – представників відокремлених підрозділів (філій) державних установ	26
5.2.5 Ідентифікація та автентифікація фізичних осіб – підприємців, які особисто звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі).....	29
5.2.6 Ідентифікація та автентифікація самозайнятих осіб, які особисто звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі).....	29

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)	30
5.2.8 Ідентифікація та автентифікація фізичних осіб, які звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі)	31
5.2.9 Ідентифікація та автентифікація фізичних осіб - нерезидентів, які звертаються до Центру із заявою про реєстрацію (Заявники – Підписувачі).....	32
5.3 Ідентифікація та автентифікація Заявників під час подання заяв на скасування, блокування та поновлення сертифікатів.....	32
5.4 Підтвердження володіння Підписувачем особистим ключем, відповідний якому відкритий ключ надається для сертифікації.....	33
5.5 Ідентифікація та автентифікація Підписувачів при повторному формуванні сертифіката	33
6 УМОВИ, ПРОЦЕДУРИ ТА МЕХАНІЗМИ, ПОВ'ЯЗАНІ З ОБСЛУГОВУВАННЯМ ТА ВИКОРИСТАННЯМ СЕРТИФІКАТІВ КЛЮЧІВ.....	34
6.1 Подання запиту на сертифікацію та оброблення запиту	34
6.2 Надання сформованого сертифіката ключа Підписувачу та визнання сертифіката його власником	35
6.3 Публікація сформованого сертифіката ключа Центром	35
6.4 Використання сертифіката ключа та особистого ключа Підписувачем та сертифіката ключа Користувачем	35
6.5 Скасування сертифіката ключа	35
6.6 Блокування сертифіката ключа	36
6.7 Поновлення сертифіката ключа.....	38
6.8 Закінчення строку чинності сертифіката ключа Підписувача	38
8 УПРАВЛІННЯ КЛЮЧАМИ.....	39
8.2 Генерація ключів Підписувачів	39

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 відкритих ключів 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 посиленних 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;

безконтактний електронний носій (БЕН) – безконтактна інтегральна схема, яка імплантована в паспорт громадянина України, призначена для внесення персональних даних, параметрів, у тому числі біометричних, що дає змогу здійснювати комплекс заходів, пов'язаних з верифікацією особи, є захищеним носієм особистих ключів та надійним засобом ЕЦП і шифрування та використовується з метою здійснення комплексу заходів, пов'язаних з ідентифікацією особи, генерацією відкритих та особистих ключів та накладанням ЕЦП, шифруванням;

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 особистих ключів – 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 даним акредитованим центром сертифікації ключів;

посилений сертифікат відкритого ключа - сертифікат ключа, який відповідає вимогам Закону України «Про електронний цифровий підпис», виданий акредитованим центром сертифікації ключів;

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 Законом України «Про електронний цифровий підпис»;

представництва – відокремлені пункти реєстрації акредитованого центру сертифікації ключів, які здійснюють реєстрацію Підписувачів та їх подальше обслуговування на відповідній території, а також треті особи, які в установленому порядку здійснюють представництво акредитованого центру сертифікації ключів Міністерства внутрішніх справ України 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, 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;
- Порядку внесення засобів електронного цифрового підпису до безконтактного електронного носія, що міститься в паспорті громадянина України, та надання послуг електронного цифрового підпису з використанням паспорта громадянина України з імплантованим безконтактним електронним носієм, затвердженого постановою Кабінету Міністрів України від 30.11.2016 № 869;
- Порядку взаємодії акредитованого центру сертифікації ключів Міністерства внутрішніх справ України та Державної міграційної служби України під час надання послуг електронного цифрового підпису з використанням паспорта громадянина України з імплантованим безконтактним електронним носієм, затвердженого наказом Міністерства внутрішніх справ України від 27.03.2018 № 238, зареєстрованим в Міністерстві юстиції України 19.04.2018 за № 475/31927 (далі – Порядок взаємодії);

- 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, а також для користувачів в частині, що їх стосується.

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 Правил посиленої сертифікації та інших вимог 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.

Всі зміни та доповнення, внесені Центром до Регламенту, що не пов'язані зі зміною законодавства, набувають чинності через 10 (десять) календарних днів з дня 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. , але не раніше монету опублікування змін на електронному інформаційному ресурсі Центру

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 України, 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. Богомольця, 10.

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

Адреса розміщення центрального офісу Центру: Україна, 01024, м. Київ, вул. 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, ПІДПISУВАЧІВ 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 - окремі підрозділи або позаштатні одиниці МВС та його територіальних органів, окремі підрозділи центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України, юридичні особи, які на підставі наказу або договору з МВС 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 здійснювати в інтересах акредитованого центру сертифікації ключів відповідно до законодавства процедури, визначені актами МВС, відповідно до вимог законодавства у сфері електронного цифрового підпису.

Договори про надання послуг ЕЦП укладаються від імені МВС.

Заявниками можуть бути безпосередньо Підписувачі або юридичні особи публічного та приватного права (у тому числі їх відокремлені підрозділи, філії), які звертаються до Центру з метою формування сертифікатів для представників (керівників органів управління, посадових осіб, працівників, співробітників тощо) – Підписувачів такої 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, аудиторів, арбітражні керуючі, оцінювачі та інші);
- наймані працівники фізичних осіб – підприємців та самозайнятих осіб (приватних нотаріусів, адвокатів, аудиторів, арбітражних керуючих, оцінювачів та інших);
- фізичні особи.

Центр надає послуги ЕЦП фізичним особам - володільцям паспорта громадянина України з імплантованим БЕН, які досягли вісімнадцятирічного віку, є дієздатними, оформили паспорт громадянина України з імплантованим БЕН у встановленому законодавством порядку та виявили бажання отримувати послуги ЕЦП з використанням паспорта громадянина України з імплантованим БЕН. Надання послуг ЕЦП володільцям паспорта громадянина України з імплантованим БЕН, що використовується як захищений носій особистих ключів, при генерації першої пари ключових даних, які використовуються для накладення та перевірки ЕЦП, та першої пари ключових даних, які використовуються для протоколу узгодження ключів шифрування (далі - перші пари ключових даних), здійснюється за принципом розмежування повноважень між Центральним офісом Центру, представництвами та представниками Центру відповідно до Порядку взаємодії.

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 фізичної або юридичної 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;
- під час реєстрації вимагати від Заявників надавати повну та достовірну інформацію, необхідну для 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 (умисної дискредитації, пошкодження майна тощо);
- 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 Підписувача (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 щодо 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 більш ніж двох годин 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;

- вести облік укладених договорів із Заявниками, а також документів (посвідчених в установленому порядку копій документів), що використовуються під час реєстрації;
- надавати консультації з питань, пов'язаних з ЕЦП;
- надавати допомогу Підписувачам при здійсненні ними генерації ключів за допомогою надійних засобів ЕЦП;
- у разі надання допомоги при генерації ключів Підписувачами, вживати заходів щодо забезпечення конфіденційності;
- забезпечувати конфіденційність та цілісність особистого ключа у разі передачі ключа Підписувачу через Заявника;
- не допускати ознайомлення з особистими ключами Підписувачів та їх зберігання 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;
 - додержуватися вимог щодо використання особистого ключа, визначених законодавством у сфері ЕЦП та цим Регламентом;
 - 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 списки 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;
- генерувати перші пари відкритих та особистих ключів на БЕН, імплантованим у паспорт громадянина України, за допомогою програмних засобів робочої станції для оформлення та видачі паспортних документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус;
- генерувати відкриті та особисті ключі з використанням SIM-карти, яка є надійним засобом ЕЦП та захищеним носієм особистих ключів, у разі отримання послуг ЕЦП з використанням мобільних технологій (MobileID);»
- 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 законодавства в сфері 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 (значення ПІН1(2) та ПАК1(2) у випадку використання БЕН, імплантованого в паспорт громадянина України, як носія особистого ключа) та ключову фразу для голосової

автентифікації;

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

- виконувати вимоги цього Регламенту в частині, що його стосується;
- перед перевіркою ЕЦП здійснювати перевірку чинності сертифіката ключа Підписувача на момент накладення ним ЕЦП, з використанням інформації про статус сертифіката, наданої 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 Порядком застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності, затвердженим 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.

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, та Підписувачів – володільців паспорта громадянина України з імплантованим БЕН, на який згенеровано перші пари ключових даних;
- списки відкликаних сертифікатів, сформованих Центром;
- 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;
 - 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.

Публікація сертифікатів ключів, сформованих Підписувачу – фізичній особі, на ім'я якої оформлено паспорт громадянина України з імплантованим БЕН, на який згенеровано перші пари ключових даних, здійснюються автоматично на електронному інформаційному ресурсі Центру.

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 зміну статусу сертифіката (скасування, блокування, поновлення сертифіката);
- звернення до Центру про повторне формування сертифіката;
- звернення до Центру із заявою на зміну реквізитів 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 зміну статусу сертифіката (скасування, блокування, поновлення сертифіката);
- заяви на зміну реквізитів сертифіката.

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

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

- подання заяви щодо блокування сертифіката в електронній формі;
- здійснення Центром підтвердження володіння Підписувачем особистим ключем, відповідний якому відкритий ключ надається для сертифікації;
- подання заяви щодо 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) за допомогою засобів телекомунікаційного зв'язку;
- звернення представника Центру із заявою про реєстрацію фізичної особи, на ім'я якої оформлено паспорт громадянина України з імплантованим БЕН, як підписувача відповідно до Порядку взаємодії.

Форми заяв публікуються на електронному інформаційному ресурсі Центру.

Засобами свого електронного інформаційного ресурсу Центр може надавати можливість попередньої реєстрації Заявників для формування та обслуговування електронної черги Заявників. Реєстрація Заявників в електронній черзі не виключає зобов'язань Центру та Заявників щодо подання заяв про реєстрацію та проходження процедур ідентифікації та автентифікації за особистої присутності Заявників або осіб, уповноважених представляти їх інтереси на законних підставах.

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

Реєстрація є підставою для формування сертифіката ключа Підписувача.

Максимальний час між отриманням Центром 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;
- неунікальність наданого відкритого ключа Підписувача в реєстрі чинних, блокованих та скасованих сертифікатів.

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 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, встановлення їх належності до юридичної особи та повноважень використовуються:

- оригінали (для ознайомлення) та копії документів, що посвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані;
- копії документів, що посвідчують 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 рекомендації 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 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, встановлення їх належності до юридичної особи та повноважень використовуються:

- оригінали (для ознайомлення) та копії документів, що посвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані;
- копії документів, що посвідчують 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 рекомендацій 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 рішенням 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 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, встановлення їх належності до державної установи та повноважень 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 посвідчують 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.

Центр за допомогою системи електронної взаємодії органів виконавчої влади може здійснювати 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 рекомендації 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 рішенням 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 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 та встановлення їх повноважень використовуються:

- оригінали (для ознайомлення) та копії документів, що посвідчують 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 посвідчують 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.

Центр за допомогою системи електронної взаємодії органів виконавчої влади може здійснювати 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 з імплантованим БЕН;
- реєстраційні дані місця проживання (копія 11-16 сторінок паспорта громадянина України (за наявності відміток) або копія довідки про реєстрацію місця проживання фізичної особи/ копія витягу з Єдиного державного демографічного реєстру щодо реєстрації місця проживання).

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 посвідчують 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 та 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 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 та 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 з імплантованим БЕН;
- реєстраційні дані місця проживання (копія 11-16 сторінок паспорта громадянина

України (за наявності відміток) або копія довідки про реєстрацію місця проживання фізичної особи/ копія витягу з Єдиного державного демографічного реєстру щодо реєстрації місця проживання);

- 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 (трудоий 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);

- 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 та 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 з імплантованим БЕН

- реєстраційні дані місця проживання (копія 11-16 сторінок паспорта громадянина України (за наявності відміток) або копія довідки про реєстрацію місця проживання фізичної особи/ копія витягу з Єдиного державного демографічного реєстру щодо реєстрації місця проживання).

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 посвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані.

Копії документів засвідчуються відповідно до законодавства.

Перелік документів та рекомендації 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.

Приймання заяв про реєстрацію в Центрі як підписувачів, ідентифікація та автентифікація Підписувачів при наданні послуг ЕЦП особі, на ім'я якої оформлено паспорт громадянина України з імплантованим БЕН, при генерації на БЕН першої пари ключових даних проводиться працівниками територіальних органів та територіальних підрозділів ДМС, які здійснюють оформлення та видачу паспорта громадянина України та здійснюють представництво Центру відповідно до Порядку взаємодії.

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;
- 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 посвідчують особу Підписувача - власника відкритого ключа та підтверджують її ідентифікаційні дані (зокрема паспорт громадянина іншої країни з нотаріально засвідченим перекладом українською мовою, посвідка на тимчасове/постійне проживання, посвідчення біженця).

Копії документів засвідчуються відповідно до законодавства.

Перелік документів та рекомендації 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 щодо скасування, блокування та поновлення сертифікатів

Ідентифікація та автентифікація Заявників під час подання заяв щодо 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.

Підтвердження володіння Підписувачем особистим ключем здійснюється шляхом перевірки ЕЦП, накладеного особистим ключем Підписувача на запит на формування сертифіката (запит на сертифікацію), за допомогою відкритого ключа, що міститься у цьому запиті на сертифікацію.

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 випадку подання до Центру письмової заяви на зміну реквізитів сертифіката при зміні даних про Підписувача без генерації нового особистого ключа відповідно до пункту 5.2 цього Регламенту.

У разі повторного формування сертифіката при зміні даних про Підписувача, зазначених у сертифікаті, окрім заяви на зміну реквізитів 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 Підписувача і додаткову інформацію для формування сертифіката, який формується під час генерації особистого та відкритого ключів Підписувача надійними засобами ЕЦП.

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 про реєстрацію від осіб - Заявників, зазначених у Розділі 5 цього Регламенту, на носіїв інформації.

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

Оброблення запиту на сертифікацію здійснюється Центром, в особі адміністратора реєстрації (віддаленого адміністратора реєстрації), після ідентифікації та автентифікації особи, яка подає заяву та після підтвердження володіння Підписувачем (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.

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 про реєстрацію, становить не більше двох годин.

Подання та обробка запитів на сертифікацію для Підписувачів – володільців паспорта громадянина України з імплантованим БЕН при генерації на БЕН першої пари ключових даних здійснюється відповідно до Порядку взаємодії. Усі події, пов'язані із формуванням та відправкою запитів на реєстрацію фізичної особи, на ім'я якої оформлено паспорт громадянина України з імплантованим БЕН, як підписувача та запитів на формування сертифікатів ключів ЕЦП та шифрування, вносяться до журналу реєстрації подій Єдиної інформаційно-аналітичної системи управління міграційними процесами ДМС із забезпеченням ідентифікації ініціатора події - працівника суб'єкта, що здійснює представництво Центру, за допомогою сертифіката ключа, власником якого є вказаний працівник.

При отриманні послуг ЕЦП з використанням мобільних технологій формування та подання до Центру запитів на сертифікацію для Підписувачів - володільців SIM-карток, які є надійним засобом ЕЦП та захищеним носієм ключової інформації, здійснюється з використанням засобів інформаційно-телекомунікаційної системи постачальника послуг MobileID та виконанням вимог законодавства щодо захисту інформації.

6.2 Надання сформованого сертифіката ключа Підписувачу та визнання сертифіката його власником

Надання сформованого сертифіката ключа Підписувачу здійснюється в один із способів:

- шляхом публікації сформованого сертифіката на електронному інформаційному ресурсі Центру;
- шляхом запису файлу із сформованим сертифікатом ключа на носій інформації, наданий Заявником (на вимогу Заявника);
- шляхом надсилання файлу із сформованим сертифікатом ключа на адресу електронної пошти, вказану в заяві про реєстрацію (на вимогу Заявника);
- шляхом надання сертифіката ключа в роздрукованому вигляді (на вимогу Заявника).

Підписувач повинен перевірити свої ідентифікаційні дані, внесені до сертифіката 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 правильності даних внесених до 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 Заявнику (Підписувачу) або особі, уповноваженій представляти його інтереси на законних підставах, 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 адміністратором сертифікації, після цього долучається до особової справи Підписувача.

6.3 Публікація сформованого сертифіката ключа Центром

Сформований Центром сертифікат ключа публікуються у порядку розповсюдження (публікації) інформації Центром, встановленим розділом 4 цього Регламенту.

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;
- встановлення факту надання Центру власником ключа недостовірних даних;
- компрометації особистого ключа;
- отримання від ДМС запиту на скасування сертифіката ключа фізичної особи, на ім'я якої оформлено паспорт громадянина України з імплантованим БЕН та яка отримала в Центрі послуги ЕЦП у зв'язку з генерацією на БЕН першої пари ключових даних (скасування сертифіката ключа здійснюється відповідно до Порядку взаємодії).

Скасування блокованого сертифіката ключа здійснюється Центром автоматично, якщо протягом тридцяти календарних днів з дня блокування сертифіката ключа Підписувач (Заявник) не поновить його чинність.

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 щодо 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 щодо скасування сертифіката, а також перевірити законність такого звернення.

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

Перелік документів та рекомендації щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Максимальний час між отриманням заяви щодо 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 підозри на компрометацію особистого ключа;
- 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 щодо 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.

У випадку тимчасового вилучення паспорта громадянина України з імплантованим БЕН діючі сертифікати ключів ЕЦП та шифрування фізичної особи, на ім'я якої оформлено паспорт, блокуються шляхом подачі у встановленому порядку заяви щодо блокування сертифікатів ключів до Центру Підписувачем.

З метою забезпечення захисту особистого ключа від компрометації підписувач, на ім'я якого оформлено тимчасово вилучений паспорт громадянина України з імплантованим БЕН, зобов'язаний не розголошувати та не повідомляти особам, якими вилучено паспорт, пароль доступу до особистого ключа (значення ПН1(2) та ПАК1(2)) та ключову фразу для голосової автентифікації.

Після блокування сертифіката ключа, Підписувач (Заявник) може протягом тридцяти календарних днів поновити чинність сертифіката ключа. Блокований сертифікат ключа буде автоматично скасований Центром, якщо протягом зазначеного строку Підписувач (Заявник) не поновить його чинність.

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

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

Перелік документів та рекомендації щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Перевірка ідентифікаційних даних Підписувача, який звертається із заявою щодо 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 щодо 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 НТТР-запиту. При цьому, заява щодо блокування сертифіката в електронному вигляді засвідчується власним ЕЦП Підписувача.

Перевірка ідентифікаційних даних особи, яка звертається із усною заявою щодо 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 щодо 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 щодо блокування сертифіката та зміною його статусу, інформація про який доступна Користувачам, не повинен перевищувати двох годин.

У разі передачі заяви щодо 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 щодо поновлення сертифіката.

Заява щодо 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 щодо поновлення сертифіката, а також перевірити законність такого звернення.

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

Перелік документів та рекомендації щодо їх оформлення публікуються на електронному інформаційному ресурсі Центру.

Максимальний час між отриманням заяви щодо 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 такого особистого ключа Підписувача, сертифікат якого нечинний – 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;
- у територіальному органі, територіальному підрозділ ДМС за допомогою засобів робочої станції для оформлення та видачі документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус;
 - з використанням SIM-карти Підписувача, яка є надійним засобом ЕЦП, захищеним носієм ключової інформації - у разі отримання послуг ЕЦП з використанням мобільних технологій (MobileID).

У разі 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.

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

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.

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

У разі генерації перших пар ключових даних на БЕН, імплантований у паспорт громадянина України, генерація таких пар здійснюється фізичною особою, на ім'я якої оформлено паспорт громадянина України з імплантованим БЕН, у територіальному органі, територіальному підрозділ ДМС за допомогою програмних засобів робочої станції для оформлення та видачі документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус, з комплектом обладнання для зняття біометричних даних (параметрів) і реєстрації/зняття з реєстрації місць проживання/перебування громадян України, іноземців та осіб без громадянства.

У разі генерації чергових пар ключових даних на БЕН, імплантований у паспорт громадянина України, фізична особа, на ім'я якої оформлено цей паспорт, самостійно із використанням надійних засобів ЕЦП, наданих Центром генерує ключові дані. Центр та

суб'єкти, що здійснюють представництво Центру, можуть надавати допомогу в генерації на БЕН чергових пар ключових даних в офісах у разі їх особистого відвідування фізичними особами, на ім'я яких оформлено паспорт громадянина України з імплантованим БЕН.

У разі генерації ключових даних з використанням SIM-карти така генерація здійснюється Підписувачем самостійно після ідентифікації SIM-карти у постачальника послуг MobileID та отримання від Центру запиту на генерацію ключових даних Підписувача. На підставі відкритих ключів, отриманих з SIM-карти, а також ідентифікаційних даних Підписувача віддалений адміністратор реєстрації Центру, що здійснює надання послуг ЕЦП з використанням технології MobileID, створює запити на сертифікацію, що подаються до Центру.

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

Згенерований особистий ключ Підписувача захищається паролем та записується на носій ключової інформації (далі- 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.

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.