Прим. № __

ПОГОДЖЕНО
Перший заступник Голови
Державної служби спеціального
зв`язку та захисту інформації
України
_____ О.М. Чаузов
« 8 » 09 2018 р.

ЗАТВЕРДЖУЮ
Генеральний директор
державного підприємства
«Національні інформаційні системи»
_____ С.С. Лур'є
« 7 » 09 2018 р.

РЕГЛАМЕНТ РОБОТИ

АКРЕДИТОВАНОГО ЦЕНТРУ СЕРТИФІКАЦІЇ КЛЮЧІВ ОРГАНІВ ЮСТИЦІЇ УКРАЇНИ

На 57 аркушах

(нова редакція)

ПОГОДЖЕНО
Заступник директора департаменту - начальник акредитованого центру сертифікації ключів Департаменту систем електронного цифрового підпису та електронної ідентифікації державного підприємства «Національні інформаційні системи»
_____ Д.М. Гук
« 03 » 08 2018 р.

ПОГОДЖЕНО
Директор Департаменту систем електронного цифрового підпису та електронної ідентифікації державного підприємства «Національні інформаційні системи»
_____ Ю.М. Козлов
« 03 » 08 2018 р.

Київ 2018 р.

ЗМІСТ

ВСТУП 5
Терміни та визначення 5
Статус Регламенту 7
Внесення змін та доповнень до Регламенту 8
1 ЗАГАЛЬНІ ПОЛОЖЕННЯ 10
2 ФУНКЦІЇ, ПРАВА ТА ОБОВ'ЯЗКИ ЦЕНТРУ, ЗАЯВНИКІВ, ПІДПИСУВАЧІВ ТА КОРИСТУВАЧІВ 11
2.1 Перелік суб'єктів, задіяних в обслуговуванні та використанні сертифікатів ключів 11
2.2 Функції, права та обов'язки Центру 12
2.3 Функції, права та обов'язки Заявників, Підписувачів, Користувачів 15
3 СФЕРИ ВИКОРИСТАННЯ ТА ОБМЕЖЕННЯ ЩОДО ВИКОРИСТАННЯ СЕРТИФІКАТІВ КЛЮЧІВ 17
4 ПОРЯДОК РОЗПОВСЮДЖЕННЯ (ПУБЛІКАЦІЇ) ІНФОРМАЦІЇ ЦЕНТРОМ 17
4.1 Перелік інформації, що публікується Центром 17
4.2 Час і порядок публікації сертифікатів та списків відкликаних сертифікатів 18
5 ПОРЯДОК ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ 18
5.1 Загальні положення 18
5.2 Ідентифікація та автентифікація Заявників та Підписувачів під час подання заяв про реєстрацію 19
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 20
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... 22
5.2.3 Ідентифікація та автентифікація державних установ та фізичних осіб – представників державних установ 23
5.2.4 Ідентифікація та автентифікація відокремлених підрозділів (філій) державних установ та фізичних осіб – представників відокремлених підрозділів (філій) державних установ 25
5.2.5 Ідентифікація та автентифікація фізичних осіб – підприємців, які особисто звертаються до Центру із заявою про реєстрацію 28
5.2.6 Ідентифікація та автентифікація самозайнятих осіб, які особисто звертаються до Центру із заявою про реєстрацію 28
5.2.7 Ідентифікація та автентифікація фізичних осіб - найманих працівників самозайнятих осіб, які звертаються до Центру із заявою про реєстрацію 29
5.2.8 Ідентифікація та автентифікація фізичних осіб, які звертаються до Центру із заявою про реєстрацію 29

5.2.9 Ідентифікація та автентифікація фізичних осіб - нерезидентів, які звертаються до Центру із заявою про реєстрації……30

5.3 Ідентифікація та автентифікація Заявників під час подання заяв на скасування, блокування та поновлення сертифікатів 31

5.4 Підтвердження володіння Підписувачем особистим ключем, відповідний якому відкритий ключ надається для сертифікації 31

5.5 Ідентифікація та автентифікація Підписувачів при повторному формуванні сертифіката 31

5.5.1 Ідентифікація та автентифікація Підписувачів у випадку подання до Центру електронної заяви на повторне формування сертифіката після генерації нового особистого ключа……31

5.5.2 Ідентифікація та автентифікація Підписувачів у випадку подання до Центру письмової заяви на повторне формування сертифіката при зміні даних про Підписувача без генерації нового особистого ключа……32

6 УМОВИ, ПРОЦЕДУРИ ТА МЕХАНІЗМИ, ПОВ'ЯЗАНІ З ОБСЛУГОВУВАННЯМ ТА ВИКОРИСТАННЯМ СЕРТИФІКАТІВ КЛЮЧІВ 32

6.1 Подання запиту на сертифікацію та оброблення запиту 32

6.2 Надання сформованого сертифіката ключа Підписувачу та визнання сертифіката його власником 33

6.3 Публікація сформованого сертифіката ключа Центром 34

6.4 Використання сертифіката ключа та особистого ключа Підписувачем та сертифіката ключа Користувачем 34

6.5 Скасування сертифіката ключа 34

6.6 Блокування сертифіката ключа 35

6.7 Поновлення сертифіката ключа 36

6.8 Закінчення строку чинності сертифіката ключа Підписувача 37

7 УПРАВЛІННЯ ТА ОПЕРАЦІЙНИЙ КОНТРОЛЬ 37

7.1 Фізичне середовище 37

7.2 Процедурний контроль 37

7.2.1 Склад обслуговуючого персоналу Центру 37

7.2.2 Функції та обов’язки керівника Центру 38

7.2.3 Функції та обов’язки адміністратора безпеки 39

7.2.4 Функції та обов’язки системного адміністратора 40

7.2.5 Функції та обов’язки адміністратора сертифікації 40

7.2.6 Функції та обов’язки адміністратора реєстрації 41

7.2.7 Функції та обов’язки віддаленого адміністратора реєстрації 41

7.2.8 Функції та обов’язки відповідального за захист інформації на відокремленому пункті реєстрації 42

7.2.9 Функції та обов’язки оператора реєстрації представництва……..44

7.3 Ведення журналів аудиту автоматизованої системи Центру 43
7.4 Ведення архівів 44
8 УПРАВЛІННЯ КЛЮЧАМИ 45
8.1 Процес, порядок та умови генерації ключів Центру 45
8.2 Генерація ключів Підписувачів 45
9 ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ОСОБИСТИХ КЛЮЧІВ ЦЕНТРУ 47

ВСТУП

Терміни та визначення

У цьому Регламенті терміни та визначення вживаються у такому значенні:

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

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

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

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

блокування сертифіката ключа - тимчасове зупинення чинності сертифіката ключа;

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

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

електронний цифровий підпис - 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 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 Закону України «Про електронний цифровий підпис»;

представництва – відокремлені пункти реєстрації, що представлені окремими підрозділами або позаштатними одиницями ДП «НАІС» та його філій, які підпорядковані головному офісу Центру; або юридичні чи фізичні особи, які здійснюють представництво ДП «НАІС» в порядку, передбаченому Цивільним кодексом України, при укладанні договорів про надання послуг електронного цифрового підпису і уповноважені здійснювати в інтересах акредитованого центру сертифікації ключів процедур допомоги при генерації ключів, реєстрації та консультацій Заявників з дотриманням вимог законодавства у сфері ЕЦП та захисту інформації;

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 січня 2005 р, №3 (у редакції наказу ДСТСЗІ Служби безпеки України від 10 травня 2006 року № 50) та зареєстровано в Міністерстві юстиції України від 27 січня 2005 року 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;

уповноважений представник (особа) - член органу управління юридичної особи та інша особа, яка відповідно до закону чи установчих документів виступає від імені юридичної особи та уповноважена на її представництво в правовідносинах з третіми особами;

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 Цивільному кодексі України, 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.

Статус Регламенту

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

Регламент розроблений відповідно до:

- Закону України від 22 травня 2003 року № 852- IV “Про електронний цифровий підпис”;
- Закону України від 22 травня 2003 року № 851 - IV “Про електронні документи та електронний документообіг”;

- Закону України від 15 травня 2003 року № 755 - IV “Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань”;

- Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу, затвердженого постановою Кабінету Міністрів України від 26 травня 2004 року № 680;

- Порядку акредитації центру сертифікації ключів, затвердженого постановою Кабінету Міністрів України від 13 червня 2004 року № 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 жовтня 2004 року № 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) та зареєстрованих в Міністерстві юстиції України за № 568/12442 від 17.05.2006;

- Вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису, затверджених Наказом Міністерства юстиції України, Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 20.08.2012 № 1236/5/453, зареєстрованих в Міністерстві юстиції України 20 серпня 2012 року за номером 1398/21710;

- 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.

Визнання вимог Регламенту Заявниками, Підписувачами та Користувачами послуг ЕЦП обов’язковими є умовою та підставою для укладання з ними договору про надання послуг ЕЦП.

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

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

Внесення змін та доповнень до Регламенту

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

Про внесення змін та доповнень до цього Регламенту, Центр повідомляє Заявників, Підписувачів, Користувачів послуг ЕЦП та інших зацікавлених осіб шляхом розміщення

зазначених змін та доповнень на електронному інформаційному ресурсі Центру, а також шляхом розсилання повідомлень засобами електронної пошти.

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

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

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

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

Центр має такі ідентифікаційні дані.

Повні найменування юридичної особи: державне підприємство «Національні інформаційні системи», State enterprise «National information systems».

Скорочені найменування юридичної особи: ДП «НАІС», State enterprise «NAIS».

Повні найменування Центру: Акредитований центр сертифікації ключів органів юстиції України, Certification Authority of the Justice of Ukraine.

Скорочені найменування Центру: АЦСК органів юстиції України, CA of the Justice of Ukraine.

Юридична адреса: Україна, 04053, м. Київ, вул. Січових Стрільців, 73.

Поштова адреса головного офісу Центру: Україна, 04053, м. Київ, вул. Бульварно - Кудрявська, 4.

Адреса розміщення головного офісу Центру: Україна, 04053, м. Київ, вул. Бульварно - Кудрявська, 4.

Телефон: +38 (044) 206-71-59.

Код ЄДРПОУ: 39787008.

Електронна адреса інформаційного ресурсу Центру: ca.informjust.ua

Адреса електронної пошти головного офісу Центру: ca@informjust.ua

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

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

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

- Центр у складі:
  - головного офісу Центру;
  - представництв;
- Заявники;
- Підписувачі;
- Користувачі.

Головний офіс Центру представлений окремим підрозділом або позаштатною структурою ДП «НАІС», що здійснює надання послуг ЕЦП та забезпечує виконання вимог законодавства до акредитованих центрів сертифікації ключів.

Представництвами є:

- відокремлені пункти реєстрації, що представлені окремими підрозділами або позаштатними одиницями ДП «НАІС» та його філій, які підпорядковані головному офісу Центру, або юридичні чи фізичні особи, які на підставі договору з ДП «НАІС», здійснюють реєстрацію Підписувачів з дотриманням вимог законодавства у сфері ЕЦП та захисту інформації;

Договори про надання послуг ЕЦП укладаються від імені ДП «НАІС» або від імені представництва.

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, підприємства, установи та організації державної форми власності (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);
- самозайняті особи (приватні нотаріуси, адвокати, аудитори, арбітражні керуючі, оцінювачі та інші);
- наймані працівники самозайнятих осіб (приватних нотаріусів, адвокатів, аудиторів, арбітражних керуючих, оцінювачів та інших);
- фізичні особи.

2.2 Функції, права та обов'язки Центру

2.2.1 Центр має право:

- отримувати та перевіряти інформацію, необхідну для реєстрації Підписувачів і формування посилених сертифікатів ключів, безпосередньо у юридичної або фізичної особи чи її представника;
- надавати послуги ЕЦП в обсягах, передбачених законодавством та на підставі укладених договорів, у тому числі:
  - надання у користування засобів ЕЦП;
  - надання допомоги при генерації відкритих та особистих ключів;
  - обслуговування сертифікатів ключів (реєстрація Підписувачів, формування, розповсюдження, скасування, зберігання, блокування та поновлення сертифікатів ключів);
  - надання інформації щодо чинних, скасованих і блокованих посилених сертифікатів ключів;
  - послуги фіксування часу;
  - консультації з питань ЕЦП;
  - інші послуги, які не суперечать вимогам законодавства;
- обслуговувати виключно посилені сертифікати ключів;
- вимагати від Заявників надавати повну та достовірну інформацію, необхідну для реєстрації Підписувачів та формування сертифікатів ключів, а також здійснювати перевірку наданої інформації;
- скасовувати, блокувати, поновлювати сертифікати ключів Підписувачів у порядку, визначеному цим Регламентом;
- вимагати від Підписувачів дотримуватись вимог цього Регламенту та умов договору про надання послуг;
- вимагати від Заявників зобов'язувати Підписувачів дотримуватись вимог цього Регламенту та умов договору про надання послуг;
- здійснювати переформування сертифіката Підписувачу із використанням попередньо засвідченого відкритого ключа Підписувача у разі, якщо відповідний йому особистий ключ не був скомпрометований, та з дотриманням вимог щодо недопущення перевищення часу чинності особистого ключа та відповідного йому відкритого ключа більше двох років;
- припинити надання послуг ЕЦП Підписувачеві у разі порушення ним істотних умов договору про надання послуг ЕЦП та умов цього Регламенту;
- вимагати від Заявників та Підписувачів відшкодування в повному обсязі майнової та моральної шкоди у разі, якщо така шкода була завдана Центру з вини Заявників та Підписувачів;
- укладати договір із Заявником про надання послуг ЕЦП у формі електронного документа.

2.2.2 Центр зобов'язаний:

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

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

- використовувати для надання послуг електронного цифрового підпису 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 на вимогу Підписувача;

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

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

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

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

- забезпечувати резервування усіх сформованих сертифікатів;

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

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

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

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

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

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

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

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

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

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

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

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

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

- здійснювати генерацію ключів Підписувачам за допомогою надійних засобів ЕЦП;

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

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

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

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

  · положень політики сертифікації;

  · обмежень при використанні сертифіката ключа;

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

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

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

  · порядку розв'язання спорів;

  · законодавства в сфері ЕЦП;

  · підстав відповідальності Центру;

- зобов'язати Заявника виконувати такі основні вимоги:

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

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

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

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

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

  · не використовувати особистий ключ у разі його компрометації.

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

2.3.1 Заявник та Підписувач мають право:

- своєчасно отримувати якісні послуги ЕЦП;
- одержувати сертифікати ключів Центру;
- одержувати списки відкликаних сертифікатів, сформованих Центром;
- застосовувати сертифікат Центру для перевірки справжності ЕЦП сертифікатів, сформованих Центром;
- застосовувати список відкликаних сертифікатів, сформованих Центром, та протокол інтерактивного визначення статусу сертифіката (OCSP) для перевірки статусу власного сертифіката та сертифікатів інших Підписувачів;
- генерувати відкриті та особисті ключі на своєму робочому місці з використанням надійного засобу ЕЦП, який надається Центром;

- ознайомлюватись з інформацією щодо діяльності Центру та надання послуг ЕЦП;
- подавати заяви, скарги, претензії;
- вимагати скасування, блокування або поновлення свого сертифіката ключа.
- вимагати від Центру усунення порушень умов даного Регламенту та договору про надання послуг ЕЦП;
- вимагати від Центру виконання вимог конфіденційності;
- оскаржувати дії чи бездіяльність Центру у судовому порядку.

2.3.2 Заявник та Підписувач зобов'язані:

- ознайомитись та дотримуватись правил надання послуг ЕЦП, вимог цього Регламенту та договору про надання послуг ЕЦП;
- надавати повну та дійсну інформацію під час реєстрації, необхідну для формування посиленого сертифіката ключа;
- використовувати особистий ключ відповідно до призначення ключа, зазначеному у сертифікаті відкритого ключа, а також додержуватися інших вимог щодо його використання, визначених Центром у цьому Регламенті;
- використовувати надійні засоби ЕЦП для генерації особистих та відкритих ключів, формування та перевірки ЕЦП;
- негайно інформувати Центр про події, що трапилися до закінчення строку чинності сертифіката, а саме: втрату або компрометацію особистого ключа, втрату контролю щодо особистого ключа через компрометацію пароля, коду доступу до нього тощо, виявлену неточність або зміну даних, зазначених у посиленому сертифікаті ключа;
- не використовувати особистий ключ у разі його компрометації.
- зберігати в таємниці особистий ключ та приймати всі можливі заходи для запобігання його втрати, розкриття, копіювання, перекручування та несанкціонованого використання;
- не розголошувати та не повідомляти іншим особам пароль доступу до особистого ключа та ключову фразу для голосової автентифікації;
- не використовувати особистий ключ, відповідний до сертифіката, заява на скасування чи блокування якого подана до Центру, протягом часу з моменту подання заяви і до моменту офіційного повідомлення про скасування сертифіката;
- не використовувати особистий ключ, відповідний до сертифіката, що скасований або блокований.

2.3.3 Користувач має право:

- одержувати сертифікати ключів Центру;
- одержувати сертифікати ключів Підписувачів у разі надання ними згоди на публікацію або використання сертифікатів;
- одержувати списки відкликаних сертифікатів, сформованих Центром;
- застосовувати сертифікат Центру для перевірки справжності ЕЦП сертифікатів, сформованих Центром;

- застосовувати список відкликаних сертифікатів, сформованих Центром, та протокол інтерактивного визначення статусу сертифіката (OCSP) для перевірки статусу сертифікатів Підписувачів;
- використовувати надійні засоби ЕЦП, надані Центром, для перевірки ЕЦП;
- ознайомлюватись з інформацією щодо діяльності Центру та надання послуг ЕЦП;
- отримувати послуги ЕЦП на правах Заявника та Підписувача;
- подавати заяви, скарги, претензії;
- вимагати від Центру усунення порушень умов даного Регламенту;
- оскаржувати дії чи бездіяльність Центру у судовому порядку.

2.3.4 Користувач зобов'язаний:

- перед перевіркою ЕЦП здійснювати перевірку чинності сертифіката ключа Підписувача на момент накладення ним ЕЦП, з використанням інформації про статус сертифіката, наданою Центром;
- враховувати усі визначені у сертифікатах ключів вимоги щодо сфери та обмежень їх використання.

3 СФЕРИ ВИКОРИСТАННЯ ТА ОБМЕЖЕННЯ ЩОДО ВИКОРИСТАННЯ СЕРТИФІКАТІВ КЛЮЧІВ

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

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;
- списки відкликаних сертифікатів, сформованих Центром;
- інформація щодо умов, пов'язаних з обслуговування 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 електронного цифрового підпису;

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

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

· порядок розв'язання спорів;

· вимоги законодавства в сфері електронного цифрового підпису;

· підстави відповідальності Центру;

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

4.2 Час і порядок публікації сертифікатів та списків відкликаних сертифікатів

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

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

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

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

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

5 ПОРЯДОК ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

5.1 Загальні положення

Ідентифікація та автентифікація Заявників та Підписувачів здійснюється Центром у випадках:

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

Ідентифікація здійснюється за ідентифікаційними даними, визначеними цим Регламентом.

Під час ідентифікації перевірка інформації, необхідної для реєстрації і формування сертифіката ключа Підписувачів здійснюється Центром виключно за їх особистою присутності відповідно статті 5 Закону України від 22 травня 2003 року № 852- IV “Про електронний цифровий підпис” (зі змінами), якщо інше не встановлено цим Законом.

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 ДП «НАІС», у випадках подання:

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

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

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

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

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

Реєстрація Підписувачів здійснюється Центром у випадках:

- особистого звернення фізичних осіб, у тому числі, фізичних осіб-підприємців, самозайнятих осіб та їх найманих працівників, фізичних осіб-нерезидентів із заявою про реєстрацію;
- особистого звернення фізичних осіб – представників юридичних осіб із заявою про реєстрацію;
- звернення представників відповідальних підрозділів або спеціально визначених працівників державних установ із заявою про реєстрацію працівників державної установи за допомогою засобів телекомунікаційного зв'язку.

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 на реєстрацію та проходження процедур ідентифікації та автентифікації.

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

Реєстрація є підставою для формування сертифіката ключа Підписувача.

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

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

Підстави відмови у наданні послуг ЕЦП:

- відсутність всіх документів, або інших відомостей, у тому числі в електронній формі, необхідних для ідентифікації та автентифікації Заявників та Підписувачів;
- подання документів, що мають підчистки, дописки, закреслені слова, інші незастережні та не засвідчені особистим підписом Підписувача виправлення, написи олівцем або мають пошкодження, внаслідок чого їх текст неможливо прочитати;
- подання неналежно засвідчених копій документів;
- встановлення невідповідності даних, що визначені наданими документами, або іншими відомостями, у тому числі в електронній формі, фактичним даним.

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

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

Ідентифікація юридичних осіб здійснюється за такими ідентифікаційними даними:

- найменування юридичної особи згідно з Єдиним державним реєстром юридичних осіб, фізичних осіб – підприємців та громадських формувань (далі – Єдиний державний реєстр);
- місцезнаходження юридичної особи (область, населений пункт) згідно з Єдиним державним реєстром;
- ідентифікаційний код згідно з Єдиним державним реєстром;
- 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, здійснюється за такими ідентифікаційними даними:

- прізвище, ім’я, по батькові (за наявності);
- реєстраційний номер облікової картки платника податків;
- серія та номер паспорта громадянина України - 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 власників паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій;

- займана посада по відношенню до юридичної особи, яку представляє фізична особа (у разі вимоги Заявника щодо внесення таких даних до сертифіката).

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 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 або копії установчих документів юридичної особи (для ознайомлення), що підтверджують її ідентифікаційні дані, або інші відомості в електронній формі згідно з Єдиним державним реєстром відповідно до Закону України від 15 травня 2003 року № 755 - IV “Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань”.

Для автентифікації фізичних осіб використовуються:

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

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

- копії документів, що підтверджують повноваження керівника юридичної особи;

- копії документів, що підтверджують повноваження (займану посаду) Підписувача - власника відкритого ключа (у разі вимоги Заявника щодо внесення таких даних до сертифіката) .

Автентифікація (встановлення) юридичної особи та отримання даних щодо уповноваженого 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).

Автентифікація (встановлення) юридичної особи - нерезидента та фізичних осіб - нерезидентів – представників юридичної особи – нерезидента здійснюється за тими самими правилами з урахуванням особливостей форматів ідентифікаційних даних юридичних осіб та фізичних осіб, прийнятих у державі нерезидента, які підтверджено офіційними документами, наданими підписувачем.

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

Копії документів засвідчуються відповідно до законодавства.

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

Для укладання договорів про надання послуг ЕЦП Центр може отримувати від Заявників документи, 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

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

- найменування юридичної особи згідно з Єдиним державним реєстром;
- найменування відокремленого підрозділу (філії) юридичної особи згідно з Єдиним державним реєстром;
- місцезнаходження юридичної особи (область, населений пункт) згідно з Єдиним державним реєстром;
- місцезнаходження відокремленого підрозділу (філії) юридичної особи (область, населений пункт) згідно з Єдиним державним реєстром;
- 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, здійснюється за такими ідентифікаційними даними:

- прізвище, ім’я, по батькові (за наявності);
- реєстраційний номер облікової картки платника податків;
- серія та номер паспорта громадянина України - 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 власників паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій;
- займана посада по відношенню до відокремленого підрозділу (філії) юридичної особи, який представляє фізична особа (у разі вимоги Заявника щодо внесення таких даних до сертифіката).

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 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 або копії установчих документів відокремленого підрозділу (філії) юридичної особи (для ознайомлення), що підтверджують її ідентифікаційні дані, або інші відомості в електронній формі згідно з Єдиним державним реєстром відповідно до Закону України від 15 травня 2003 року № 755 - IV “Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань”.

Для автентифікації фізичних осіб використовуються:

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

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

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

- копії документів, що підтверджують повноваження (займану посаду) Підписувача - власника відкритого ключа (у разі вимоги Заявника щодо внесення таких даних до сертифіката).

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.

Автентифікація (встановлення) відокремленого підрозділу (філії) юридичної особи - нерезидента та фізичних осіб – нерезидентів - представників відокремленого підрозділу (філії) юридичної особи – нерезидента здійснюється за тими самими правилами з урахуванням особливостей форматів ідентифікаційних даних юридичних осіб та фізичних осіб, прийнятих у державі нерезидента, які підтверджено офіційними документами, наданими підписувачем.

Копії документів засвідчуються відповідно до законодавства.

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

Для укладання договорів про надання послуг ЕЦП Центр може отримувати від Заявників документи, 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 цієї установи.

Ідентифікація державних установ здійснюється за такими ідентифікаційними даними:

- найменування державної установи згідно з Єдиним державним реєстром;
- місцезнаходження державної установи (область, населений пункт) згідно з Єдиним державним реєстром;
- 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;
- серія та номер паспорта громадянина України - 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 власників паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій.

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 в електронній формі згідно з Єдиним державним реєстром 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 даних щодо уповноваженого представника державної установи з категорії осіб, які обираються (призначаються) до органу управління державної установи, уповноважених представляти державну установу в правовідносинах з третіми особами, або осіб, які мають право вчиняти дії від імені державної установи без довіреності, у тому числі підписувати договори, а також дані про наявність обмежень щодо представництва від імені державної установи, здійснюється з використанням інформації з інформаційного ресурсу Єдиного державного реєстру.

Для автентифікації фізичних осіб використовуються:

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

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

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

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

Відповідно до Порядку, Центр за допомогою засобів телекомунікаційного зв'язку здійснює обмін інформацією, у тому числі ідентифікаційними даними для подальшої реєстрації Підписувачів, з представником відповідального підрозділу або спеціально визначеним працівником державної установи, відповідальним за застосування електронного цифрового підпису, із дотриманням вимог щодо забезпечення цілісності та конфіденційності інформації, із використанням надійних засобів електронного цифрового підпису 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 електронного цифрового підпису.

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 електронного цифрового підпису, здійснюється виключно за його особистої присутності у представництві Центру.

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

Копії документів засвідчуються відповідно до законодавства.

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

Для укладання договорів про надання послуг ЕЦП Центр може отримувати від Заявників інші документи, 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 електронного цифрового підпису в установі забезпечує підрозділ інформаційних технологій, а у разі відсутності такого - підрозділ, що виконує відповідні функції (далі - відповідальний підрозділ), або працівник, спеціально визначений наказом рішенням цієї установи.

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

- найменування державної установи згідно з Єдиним державним реєстром;
- найменування відокремленого підрозділу (філії) державної установи згідно з Єдиним державним реєстром;
- місцезнаходження державної установи (область, населений пункт) згідно з Єдиним державним реєстром;
- місцезнаходження відокремленого підрозділу (філії) державної установи (область, населений пункт) згідно з Єдиним державним реєстром;
- 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;
- серія та номер паспорта громадянина України - 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 власників паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій.

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 відокремлених підрозділів (філій) державної установи (для ознайомлення), що підтверджують її ідентифікаційні дані, або інші відомості в електронній формі згідно з Єдиним державним реєстром 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 використовуються:

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

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

- копії документів, або інші відомості, у тому числі в електронній формі, що підтверджують повноваження керівника 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 електронного цифрового підпису в установі (надаються одноразово або у разі виникнення змін);

Відповідно до Порядку, Центр за допомогою засобів телекомунікаційного зв’язку здійснює обмін інформацією, у тому числі ідентифікаційними даними для подальшої реєстрації Підписувачів, з представником відповідального підрозділу або спеціально визначеним працівником відокремленого підрозділу (філії) державної установи, відповідальним за застосування електронного цифрового підпису, із дотриманням вимог щодо забезпечення цілісності та конфіденційності інформації, із використанням надійних засобів електронного цифрового підпису 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 електронного цифрового підпису.

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 електронного цифрового підпису, 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

Ідентифікація фізичних осіб – підприємців здійснюється у порядку, встановленому пунктом 5.2.8 цього Регламенту.

5.2.6 Ідентифікація та автентифікація самозайнятих осіб, які особисто звертаються до Центру із заявою про реєстрацію

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;
- серія та номер паспорта громадянина України - 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 власників паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій;
- адреса розташування робочого місця **(**область, населений пункт) згідно з інформацією з державних інформаційних систем (реєстрів, баз даних тощо);
- 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 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, передбачені законодавством.

5.2.7 Ідентифікація та автентифікація фізичних осіб - найманих працівників самозайнятих осіб, які звертаються до Центру із заявою про реєстрацію

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 самозайнятих осіб здійснюється за такими ідентифікаційними даними:

- прізвище, ім'я, по батькові (за наявності);
- реєстраційний номер облікової картки платника податків;
- серія та номер паспорта громадянина України - 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 власників паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій;
- займана посада по відношенню до працедавця, яку представляє фізична особа – найманий працівник.

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

Для автентифікації фізичних осіб - найманих працівників самозайнятих осіб використовуються:

- оригінали (для ознайомлення) та копії документів, що підтверджують повноваження найманого працівника (Підписувача - власника відкритого ключа) та працедавця (трудовий договір (контракт));
- 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, передбачені законодавством.

5.2.8 Ідентифікація та автентифікація фізичних осіб, які звертаються до Центру із заявою про реєстрацію

Ідентифікація фізичних осіб здійснюється за такими ідентифікаційними даними:

- прізвище, ім'я, по батькові (за наявності);
- реєстраційні дані місця проживання (область, населений пункт);
- реєстраційний номер облікової картки платника податків;

- серія та номер паспорта громадянина України - 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 власників паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій.

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

Для автентифікації фізичних осіб використовуються :

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

Копії документів засвідчуються відповідно до законодавства.

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

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

5.2.9 Ідентифікація та автентифікація фізичних осіб - нерезидентів, які звертаються до Центру із заявою про реєстрацію

Ідентифікація фізичних осіб - нерезидентів здійснюється за такими ідентифікаційними даними:

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

- реєстраційні дані місця проживання (область, населений пункт);

- 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 здійснюється за документами, що підтверджують ідентифікаційні дані фізичних осіб – нерезидентів з урахуванням особливостей форматів ідентифікаційних даних осіб, прийнятих у державі нерезидента, які підтверджено офіційними документами, наданими підписувачем. Якщо текст у документах викладений іноземною мовою, то разом з копіями таких документів надається переклад на українську мову, засвідчений нотаріально.

Для автентифікації фізичних осіб - нерезидентів використовуються :

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

Копії документів засвідчуються відповідно до законодавства.

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

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

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

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

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

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

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

Підтвердження володіння Підписувачем особистим ключем здійснюється без розкриття особистого ключа.

Умови подання запиту на сертифікацію встановлено пунктом 6.1 цього Регламенту.

5.5 Ідентифікація та автентифікація Підписувачів при повторному формуванні сертифіката

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

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

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

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

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

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

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

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

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

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

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

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

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 скомпроментований, 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

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

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

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

Належність запиту на сертифікацію Заявникові підтверджується під час особистої передачі ним запиту адміністратору реєстрації (віддаленому адміністратору реєстрації, оператору реєстрації представництва) або шляхом звіряння адреси електронної пошти,

вказаної у заяві на реєстрацію із адресою електронної пошти, яку використовував Заявник під час попередньої реєстрації Заявників в електронній черзі Заявників.

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

Оброблення запиту на сертифікацію здійснюється засобами автоматизованої системи Центру.

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

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

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

Строк оброблення запиту на сертифікацію, поданого разом із заявою на реєстрацію, становить не більше однієї години.

6.2 Надання сформованого сертифіката ключа Підписувачу та визнання сертифіката його власником

Надання сформованого сертифіката ключа Підписувачу здійснюється в один із способів:

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

Підписувач повинен перевірити свої ідентифікаційні дані, внесені до 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 сертифіката відповідного відкритого ключа.

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

У разі невідповідності ідентифікаційних даних, внесених Центром до сертифіката ключа та виявлених Центром до моменту надання сформованого сертифіката ключа

Підписувачу, посадовою особою Центру здійснюється переформування сертифіката із використанням попередньо засвідченого відкритого ключа Підписувача та з дотриманням вимог щодо недопущення перевищення часу чинності особистого ключа та відповідного йому відкритого ключа більше двох років. Посадова особа, що здійснила переформування сертифіката, складає акт, в якому зазначається дата та час скасування сертифіката, ідентифікаційні дані Підписувача, що містяться в сертифікаті та невідповідні ідентифікаційні дані Підписувача, що зазначені у заяві про реєстрацію. Акт підписується посадовою особою Центру, що здійснила переформування сертифіката, та долучається до документів (посвідчених в установленому порядку копій документів), що використовувалися під час реєстрації Підписувача.

6.3 Публікація сформованого сертифіката ключа Центром

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

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

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

6.5 Скасування сертифіката ключа

Центр негайно скасовує сформований ним сертифікат ключа у разі:

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

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

Скасований сертифікат ключа поновленню не підлягає.

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

Заява на скасування сертифіката ключа подається до Центру:

- письмово особисто Підписувачем або його уповноваженим представником за формою, яка публікується на електронному інформаційному ресурсі Центру;
- в електронній формі шляхом формування Підписувачем або його уповноваженим представником заяви на скасування сертифіката ключа із використанням особистого ключа та надійного засобу ЕЦП, наданого Центром.

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

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

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

Заява на скасування сертифіката в електронному вигляді формується за допомогою надійних засобів електронного цифрового підпису, які надаються Центром, та передаються до автоматизованої системи Центру у вигляді вкладення електронного листа або у вигляді HTTP-запиту. При цьому, заява на скасування сертифіката в електронному вигляді засвідчується ЕЦП фізичної особи або керівника . керівник юридичної особи (уповноваженого представника юридичної особи (філії) на укладення правочинів з третіми особами)

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

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

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

6.6 Блокування сертифіката ключа

Центр негайно блокує сформований ним сертифікат ключа у разі:

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

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

Заява на блокування сертифіката ключа подається до Центру:

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

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

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

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

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

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

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

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

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

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

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

Блокований сертифікат ключа може бути поновлений протягом тридцяти календарних днів. Якщо протягом зазначеного строку Підписувач не поновить його чинність, то блокований сертифікат буде автоматично скасований.

6.7 Поновлення сертифіката ключа

Центр поновлює заблокований сертифікат ключа у разі:

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

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

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

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

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

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

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

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

6.8 Закінчення строку чинності сертифіката ключа Підписувача

Строк чинності сертифікатів ключів Підписувачів становить не більше двох років.

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

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

7 УПРАВЛІННЯ ТА ОПЕРАЦІЙНИЙ КОНТРОЛЬ

7.1 Фізичне середовище

Цей розділ Регламенту не входить до обсягу положень, визначених Центром для ознайомлення Користувачами.

7.2 Процедурний контроль

7.2.1 Склад обслуговуючого персоналу Центру

До складу обслуговуючого персоналу головного офісу Центру входять працівники ДП «НАІС», на яких покладено функціональні обов'язки:

- керівника Центру;
- адміністратора безпеки;
- системного адміністратора;
- адміністратора сертифікації;
- адміністратора реєстрації.

До складу обслуговуючого персоналу відокремлених пунктів реєстрації Центру представництв (відокремлені пункти реєстрації Центру) входять працівники ДП «НАІС» та його філій, на яких покладено функціональні обов'язки:

- адміністратора реєстрації відокремленого пункту реєстрації (далі – віддалений адміністратор реєстрації);
- відповідального за захист інформації на відокремленому пункті реєстрації.

До складу обслуговуючого персоналу представництв (юридичні чи фізичні особи, які здійснюють представництво ДП «НАІС» в порядку, передбаченому Цивільним кодексом України) входять працівники або залучені особи (на умовах договорів), на яких покладено функціональні обов’язки оператора реєстрації представництва.

З метою забезпечення вирішення питань, пов'язаних із проектуванням, розробленням і модернізацією, введенням в експлуатацію, обслуговуванням і підтримкою працездатності комплексної системи захисту інформації, а також контролем за станом захищеності інформації забезпечення повноти та якісного виконання організаційних та технічних заходів із захисту інформації в Центрі створено позаштатний підрозділ служби захисту інформації.

До складу служби захисту інформації Центру входять працівники ДП «НАІС», на яких покладено функціональні обов’язки:

- керівника Центру (керівник служби захисту інформації);
- адміністратора безпеки;
- системного адміністратора;
- адміністратора сертифікації;

Відповідальні за захист інформації на відокремленому пункті реєстрації функціонально підпорядковуються керівнику служби захисту інформації.

7.2.2 Функції та обов’язки керівника Центру

В межах виконання своїх обов'язків керівник Центру відповідає за організацію та контроль процесів, направлених на забезпечення функціонування, розвитку Центру та захист інформації в інформаційно-телекомунікаційній системі Центру, а саме:

- виконання регламентних процедур з експлуатації та технічного обслуговування інформаційно-телекомунікаційної системи Центру;
- ведення електронного інформаційного ресурсу Центру;
- впровадження та забезпечення функціонування комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру;
- підтримка працездатності загальносистемного та спеціального програмного забезпечення інформаційно-телекомунікаційної системи Центру;
- забезпечення актуалізації баз даних, створюваних та оброблюваних в інформаційно-телекомунікаційній системі Центру;
- розгляд та оцінка технічних рішень щодо модернізації інформаційно-телекомунікаційної системи Центру;
- розробка та узгодження технічних завдань, проектної та експлуатаційної документації інформаційно-телекомунікаційної системи Центру та комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру;
- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру після збоїв, відмов, аварій тощо;
- супроводження будівельно-монтажних та пусконалагоджувальних робіт;
- проведення попередніх випробувань, дослідної експлуатації та введення інформаційно-телекомунікаційної системи Центру в експлуатацію;

Керівник Центру безпосередньо приймає участь та контролює процес генерації ключів Центру.

Керівник Центру представляє Центр у випадках, передбачених Регламентом роботи центрального засвідчувального органу.

Керівник Центру несе відповідальність за неналежне виконання своїх обов’язків, розголошення конфіденційної інформації, зокрема відомостей про персональні дані Заявників та Підписувачів, згідно із законом.

Інші обов’язки керівника Центру визначаються посадовими обов’язками, передбаченими розпорядчими документами ДП «НАІС» та документацією комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру.

7.2.3 Функції та обов’язки адміністратора безпеки

В межах виконання своїх обов'язків адміністратор безпеки відповідає за належне функціонування комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру.

Основними обов'язками адміністратора безпеки є:

- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру після збоїв, відмов, аварій тощо;

- участь у генерації, резервному копіюванні, знищенні, відновленні з резервної копії, контролі за використанням особистих ключів Центру, особистих ключів серверів Центру (OCSP, TSP, CMP) та особистих ключів інших засобів криптографічного захисту інформації зі складу інформаційно-телекомунікаційної системи Центру, їх належним і своєчасним знищенням;

- забезпечення режиму доступу до спеціального приміщення інформаційно-телекомунікаційної системи Центру;

- налаштування апаратних та програмних засобів зі складу інформаційно-телекомунікаційної системи Центру у частині безпеки;

- організація розмежування доступу до ресурсів інформаційно-телекомунікаційної системи Центру;

- контроль за формуванням, резервуванням та обслуговуванням сертифікатів ключів Центру, серверів Центру (OCSP, TSP, CMP), Підписувачів та формуванням списків відкликаних сертифікатів;

- забезпечення спостереження (реєстрація та аудит подій в інформаційно-телекомунікаційній системі Центру, моніторинг подій тощо) за функціонуванням комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру;

- контроль за використанням особистих ключів персоналу Центру, їх належним і своєчасним знищенням.

- контроль за формуванням сертифікатів для персоналу Центру (адміністратора сертифікації, адміністраторів реєстрації, віддалених адміністраторів реєстрації);

- ведення журналів обліку адміністратора безпеки, передбачених документацією комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру;

- участь у створенні та введенні в експлуатацію комплексної системи захисту інформації на представництвах.

Адміністратор безпеки несе відповідальність за неналежне виконання своїх обов’язків, розголошення конфіденційної інформації, зокрема відомостей про персональні дані Заявників та Підписувачів, згідно із законом.

Інші обов’язки адміністратора безпеки визначаються посадовими обов’язками, передбаченими розпорядчими документами ДП «НАІС» та документацією комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру.

7.2.4 Функції та обов’язки системного адміністратора

В межах виконання своїх обов’язків системний адміністратор відповідає за належне функціонування програмно-технічного комплексу Центру та інформаційно-телекомунікаційної системи Центру у частині, що не стосується безпеки.

Основними обов'язками системного адміністратора є:

- організація експлуатації та технічного обслуговування інформаційно-телекомунікаційної системи Центру;
- участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру;
- налаштування апаратних та програмних засобів зі складу інформаційно-телекомунікаційної системи Центру у частині, що не стосується налаштувань безпеки;
- забезпечення функціонування електронного інформаційного ресурсу Центру;
- встановлення та налагодження штатної підсистеми резервного копіювання бази даних інформаційно-телекомунікаційної системи Центру;
- забезпечення відновлення та актуалізації баз даних, створюваних та оброблюваних в інформаційно-телекомунікаційній системі Центру, внаслідок збоїв;
- ведення журналів обліку системного адміністратора, передбачених документацією комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру.

Системний адміністратор несе відповідальність за неналежне виконання своїх обов’язків, розголошення конфіденційної інформації, зокрема відомостей про персональні дані Заявників та Підписувачів, згідно із законом.

Інші обов’язки системного адміністратора визначаються посадовими обов’язками, передбаченими розпорядчими документами ДП «НАІС» та документацією комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру.

7.2.5 Функції та обов’язки адміністратора сертифікації

В межах виконання своїх обов'язків адміністратор сертифікації відповідає за формування сертифікатів ключів, списків відкликаних сертифікатів, збереження та використання особистого ключа Центру.

Основними обов'язками адміністратора сертифікації є:

- участь у генерації особистих ключів серверів Центру (OCSP, TSP, CMP) та формування сертифікатів відповідних ключів;
- формування сертифікатів для персоналу Центру (адміністратора сертифікації, адміністраторів реєстрації, віддалених адміністраторів реєстрації);
- забезпечення ведення, архівування та відновлення еталонної бази даних сформованих сертифікатів;

- забезпечення підтримки електронного інформаційного ресурсу Центру, публікацію сертифікатів ключів та списку відкликаних сертифікатів;

- забезпечення актуальності еталонних, архівних і резервних копій баз сертифікатів, що створюються в Центрі, та їх зберігання;

- ведення журналів обліку адміністратора сертифікації, передбачених документацією комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру;

Адміністратор сертифікації несе відповідальність за неналежне виконання своїх обов’язків, розголошення конфіденційної інформації, зокрема відомостей про персональні дані Заявників та Підписувачів, згідно із законом.

Інші обов’язки адміністратора сертифікації визначаються посадовими обов’язками, передбаченими розпорядчими документами ДП «НАІС» та документацією комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру.

7.2.6 Функції та обов’язки адміністратора реєстрації

В межах виконання своїх обов'язків адміністратор реєстрації відповідає за встановлення Заявників та Підписувачів під час формування, блокування, поновлення та скасування сертифікатів ключів.

Основними обов'язками адміністратора реєстрації є:

- ідентифікація та автентифікація Заявників;

- перевірка заяв на реєстрацію, скасування, блокування та поновлення сертифікатів ключів Підписувачів;

- підтвердження володіння Підписувачем особистим ключем, відповідний якому відкритий ключ надається для сертифікації;

- перевірка законності звернень про блокування, поновлення та скасування сертифікатів Підписувачів;

- надавати допомогу Підписувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вжиття заходів щодо забезпечення конфіденційності особистого ключа Підписувача під час генерації ключів;

- формування запитів на формування та зміну статусу сертифікатів ключів Підписувачів;

- надання консультацій щодо умов та порядку подання заяв на формування, скасування, блокування та поновлення сертифікатів ключів Підписувачів;

- ведення архіву Центру.

Адміністратор реєстрації несе відповідальність за неналежне виконання своїх обов’язків, розголошення конфіденційної інформації, зокрема відомостей про персональні дані Заявників та Підписувачів, згідно із законом.

Інші обов’язки адміністратора реєстрації визначаються посадовими обов’язками, передбаченими розпорядчими документами ДП «НАІС» та документацією комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру.

7.2.7 Функції та обов’язки віддаленого адміністратора реєстрації

В межах виконання своїх обов'язків віддалений адміністратор реєстрації відповідає за встановлення Заявників та Підписувачів під час формування, блокування, поновлення та скасування сертифікатів ключів.

Основними обов'язками віддаленого адміністратора реєстрації є:

- ідентифікація та автентифікація Заявників;
- перевірка заяв на формування, скасування, блокування та поновлення сертифікатів ключів Підписувачів;
- підтвердження володіння Підписувачем особистим ключем, відповідний якому відкритий ключ надається для сертифікації;
- участь у веденні реєстру Підписувачів;
- формування запитів на формування та зміну статусу сертифікатів ключів Підписувачів;
- надання консультацій щодо умов та порядку подання заяв на формування, скасування, блокування та поновлення сертифікатів ключів Підписувачів;
- ведення архіву відокремленого пункту реєстрації.

Віддалений адміністратор реєстрації несе відповідальність за неналежне виконання своїх обов’язків, розголошення конфіденційної інформації, зокрема відомостей про персональні дані Заявників та Підписувачів, згідно із законом.

Інші обов’язки віддаленого адміністратора реєстрації визначаються посадовими обов’язками, передбаченими розпорядчими документами ДП «НАІС» та документацією комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру.

7.2.8 Функції та обов’язки відповідального за захист інформації на відокремленому пункті реєстрації

В межах виконання своїх обов'язків відповідальний за захист інформації на відокремленому пункті реєстрації відповідає за належну експлуатацію комплексу засобів захисту відокремленого пункту реєстрації.

Основними обов'язками відповідального за захист інформації на відокремленому пункті реєстрації є:

- організація експлуатації та технічного обслуговування апаратних та програмних засобів відокремленого пункту реєстрації;
- участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації відокремленого пункту реєстрації;
- контроль за роботою програмного комплексу відокремленого пункту реєстрації;
- контроль за використанням особистих ключів персоналу відокремленого пункту реєстрації.

участь у створенні та введенні в експлуатацію комплексної системи захисту інформації на представництвах.

Відповідальний за захист інформації на відокремленому пункті реєстрації призначається з числа віддалених адміністраторів реєстрації.

Допускається виконання функцій відповідального за захист інформації на відокремленому пункті реєстрації системним адміністратором та адміністратором безпеки у частині, що не є в протиріч з їх аналогічними функціями по відношенню до інших складових інформаційно-телекомунікаційної системи Центру

Відповідальний за захист інформації на відокремленому пункті реєстрації несе відповідальність за неналежне виконання своїх обов’язків, розголошення конфіденційної інформації, зокрема відомостей про персональні дані Заявників та Підписувачів, згідно із законом.

Інші обов’язки відповідального за захист інформації на відокремленому пункті реєстрації визначаються посадовими обов’язками, передбаченими розпорядчими документами ДП «НАІС» та документацією комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру.

7.2.9 Функції та обов’язки оператора реєстрації представництва

В межах виконання своїх обов'язків оператор реєстрації представництва (юридичні чи фізичні особи, які здійснюють представництво ДП «НАІС» в порядку, передбаченому Цивільним кодексом України).

Основними обов'язками оператора реєстрації представництва є:

- ідентифікація та автентифікація Заявників;
- перевірка заяв на реєстрацію, скасування, блокування та поновлення сертифікатів ключів Підписувачів;
- підтвердження володіння Підписувачем особистим ключем, відповідний якому відкритий ключ надається для сертифікації;
- перевірка законності звернень про блокування, поновлення та скасування сертифікатів Підписувачів;
- надання консультаційної допомоги Підписувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вжиття заходів щодо забезпечення конфіденційності особистого ключа Підписувача під час генерації ключів;
- обслуговування запитів на формування та зміну статусу сертифікатів ключів Підписувачів та передача їх на обробку до Центру;
- надання консультацій щодо умов та порядку подання заяв на формування, скасування, блокування та поновлення сертифікатів ключів Підписувачів;
- ведення архіву Центру.

Оператор реєстрації несе відповідальність за неналежне виконання своїх обов’язків, розголошення конфіденційної інформації, зокрема відомостей про персональні дані Заявників та Підписувачів, згідно із законом.

Інші обов’язки оператора реєстрації представництва визначаються посадовими обов’язками, передбаченими розпорядчими документами юридичної особи – представництва, договірними актами з ДП «НАІС», документацією комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру.

7.3 Ведення журналів аудиту автоматизованої системи Центру

У журналах реєстрації подій (аудиту) автоматизованої системи Центру реєструються такі події:

- встановлення параметрів (налаштувань) операційних систем та програмного забезпечення;
- встановлення прав доступу та інших параметрів безпеки;
- генерація, використання та знищення ключових даних;
- внесення, модифікація та видалення реєстраційних даних Підписувачів;
- формування, блокування, скасування та поновлення сертифікатів ключів, а також формування списків відкликаних сертифікатів;

- створення резервних копій та відновлення реєстру сертифікатів та списків відкликаних сертифікатів та іншої важливої інформації;
- отримання персоналом доступу Центру та її складових частин (вхід до операційної систему тощо);
- спроби несанкціонованого доступу до автоматизованої системи Центру та її складових частин;
- збої у роботі автоматизованої системи Центру та її складових частин.

Журнали аудиту ведуться в електронній або паперовій формі, в обсягах та порядку, визначеним цим Регламентом та документацією комплексної системи захисту інформації інформаційно-телекомунікаційної системи Центру.

Захист журналів реєстрації повинен забезпечуватися засобами операційних систем та програмного забезпечення автоматизованої системи Центру або належному зберіганню у сховищах (сейфах) паперових журналів, відповідальність за що несе адміністратор безпеки.

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

Журнали реєстрації переглядаються не рідше ніж раз на добу. Перегляд журналів здійснює адміністратор безпеки. Строк зберігання реєстраційних записів аудиту – не обмежений.

7.4 Ведення архівів

Архівування інформації здійснюється згідно із внутрішніми організаційно-розпорядчими документами ДП «НАІС».

Обов'язковому архівуванню у Центрі підлягають:

- сертифікати Центру, серверів Центру (OCSP, TSP, CMP) та адміністраторів;
- сертифікати Підписувачів;
- запити на скасування, блокування та поновлення сертифікатів Підписувачів у електронному вигляді;
- журнали реєстрації подій (аудиту) автоматизованої системи Центру;
- укладені договори про надання послуг ЕЦП;
- документи та копії документів, що використовуються під час реєстрації;
- заяви на формування, скасування, блокування та поновлення сертифікатів ключів Підписувачів.

Документи у паперовому та електронному вигляді, мають зберігатися у порядку, встановленому законодавством про архіви та архівні справи. Документи, що підлягають архівному зберіганню, є документами тимчасового зберігання. Строк зберігання архівних документів – не менше трьох років.

Знищення архівних документів має здійснюватися комісією, до складу якої входять керівник Центру та адміністратор безпеки (а також, за необхідності, адміністратор сертифікації). Після завершення процедури знищення архівних документів повинен складатися відповідний акт, який затверджує керівник Центру.

Сертифікати ключів Центру, сертифікати ключів серверів Центру (OCSP, TSP, CMP) та сертифікати адміністраторів, сертифікати Підписувачів, а також списки відкликаних сертифікатів мають зберігатися постійно.

Для зберігання носіїв з резервними та архівними копіями виділяється окреме сховище (сейф чи відсік сейфу) з двома екземплярами ключів і пристроями для опечатування. Один екземпляр ключа від сховища знаходиться у адміністратора безпеки, а другий – в опечатаному вигляді зберігається у сховищі (сейфі) керівника Центру.

Засоби, що входять до складу центрального серверу автоматизованої системи Центру, забезпечують автоматичне резервне копіювання реєстру сертифікатів. Автоматичне створення резервної копії має виконуватися не рідше одного разу на добу, під час найменшого завантаження центрального серверу.

Додатково може виконуватися резервне копіювання сертифікатів на оптичні носії, або інші з’ємні носії інформації у ручному режимі. Після створення нової резервної копії, попередня резервна копія стає архівною.

Відновлення сертифікатів з резервної копії здійснюються засобами центрального сервера комплексу шляхом зчитування сертифікатів з останньої (актуальної) резервної копії та запису їх у базу даних сервера.

З’ємні носії зберігаються у конвертах чи упаковках, що опечатується печаткою адміністратора безпеки. При цьому на упаковці вказується обліковий номер копії. Факти створення та використання копій фіксуються у окремому журналі.

Архівні копії журналів реєстрації мають зберігатися в приміщенні АЦСК не менше 2-х років. Контроль за здійсненням автоматичного резервного копіювання та виконання резервного копіювання в ручному режимі покладається на системного адміністратора. Адміністратор безпеки періодично контролює процес створення та зберігання резервних копій.

Архівне приміщення обладнується технічними засобами, які виключають проникнення сторонніх осіб та неконтрольований доступ до інформації, що підлягає архівуванню.

8 УПРАВЛІННЯ КЛЮЧАМИ

8.1 Процес, порядок та умови генерації ключів Центру

Цей розділ Регламенту не входить до обсягу положень, визначених Центром для ознайомлення Користувачами в повному обсязі.

8.2 Генерація ключів Підписувачів

Особистий та відкритий ключі Підписувача може бути згенерований:

– на стаціонарному робочому місці Підписувача або на власному портативному обчислювальному пристрої;

– у надійних засобах електронного цифрового підпису у вигляді SIM-карток;

– на робочій станції генерації ключів в офісах Центру.

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

Генерація відкритого та особистого ключів у надійних засобах електронного цифрового підпису у вигляді SIM-карток Підписувача здійснюється вбудованими механізмами цих апаратно-програмних засобів. Допомога при генерації ключів у SIM-картці здійснюється адміністратором реєстрації, віддаленим адміністратором реєстрації або

оператором реєстрації представництва – працівником оператора мобільного зв’язку, який обслуговує такі засоби електронного цифрового підпису, та який виконує функції представництва Центру.

Надійні засоби електронного цифрового підпису 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 електронного цифрового підпису 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.

Надійні засоби електронного цифрового підпису у вигляді SIM-карток надаються Підписувачу Центром або оператором мобільного зв’язку, який обслуговує такі засоби, та який виконує функції представництва Центру. SIM-картки є захищеними носіями особистих ключів.

Генерація особистих ключів здійснюється з використанням захищених носіїв особистих ключів у випадках, визначених законодавством.

Згенерований особистий ключ Підписувача захищається паролем. Відповідальність за забезпечення конфіденційності та цілісності власного особистого ключа несе сам Підписувач.

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

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

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

У разі генерації відкритого та особистого ключа Підписувача у надійних засобах електронного цифрового підпису у вигляді SIM-карток, ініціювання генерації ключів у SIM-картці здійснюється оператором мобільного зв’язку, який виконує функції представництва Центру, через власну облікову систему. Згенерований особистий ключ Підписувача захищається PIN-кодом та зберігається і використовуються виключно у SIM-картці.

Надійні засоби електронного цифрового підпису у вигляді SIM-карток з використанням облікової системи оператора мобільного зв’язку під час генерації ключів також формують запит на формування сертифіката (запит на сертифікацію) формату PKCS#10, що містить відкритий ключ Підписувача і додаткову інформацію для формування сертифіката у Центрі.

Запит на сертифікацію у цьому випадку подається до Центру з системи оператора мобільного зв’язку в особі оператора реєстрації представництва Центру в автоматичному режимі каналами зв’язку.

Оброблення запитів на сертифікацію, поданих до Центру, здійснюється в автоматичному режимі 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 або на власному портативному обчислювальному пристрої Підписувача.

Для генерації відкритого та особистого ключів на робочій станції генерації ключів, що входить до складу автоматизованої системи Центру або на власному портативному обчислювальному пристрої Підписувача, застосовуються надійні засоби електронного цифрового підпису у вигляді апаратно-програмних засобів та окремих програмних додатків.

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

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

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

Особисті ключі 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.

9 ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ОСОБИСТИХ КЛЮЧІВ ЦЕНТРУ

Цей розділ Регламенту не входить до обсягу положень, визначених Центром для ознайомлення Користувачами.