КОПІЯ

МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ

НАКАЗ

29.01.2013 м. Київ № 183/5

Зареєстровано в Міністерстві юстиції України
"30" січня 2013 р.
за № 191/22723
Керівник реєструючого органу _____
підпис

Про затвердження Регламенту роботи центрального засвідчувального органу

Відповідно до підпунктів 65, 66 пункту 4 Положення про Міністерство юстиції України, затвердженого Указом Президента України від 06 квітня 2011 року № 395, Порядку акредитації центру сертифікації ключів, затвердженого постановою Кабінету Міністрів України від 13 липня 2004 року № 903, Положення про центральний засвідчувальний орган, затвердженого постановою Кабінету Міністрів України від 28 жовтня 2004 року № 1451,

НАКАЗУЮ:

1. Затвердити Регламент роботи центрального засвідчувального органу, що додається.

2. Департаменту нотаріату, банкрутства та функціонування центрального засвідчувального органу Міністерства юстиції України (Чижмарь К.І.) подати цей наказ на державну реєстрацію відповідно до Указу Президента України від 03 жовтня 1992 року № 493 «Про державну реєстрацію нормативно-правових актів міністерств та інших органів виконавчої влади».

3. Адміністратору інформаційно-телекомунікаційної системи центрального засвідчувального органу (Добжанський В.Б.) розмістити цей наказ на офіційному веб-сайті центрального засвідчувального органу.

4. Визнати таким, що втратив чинність, наказ Міністерства юстиції України від 28 вересня 2012 року № 1434/5 «Про затвердження Регламенту роботи центрального засвідчувального органу», зареєстрований у Міністерстві юстиції України 05 жовтня 2012 року за № 1692/22004.

5. Контроль за виконанням цього наказу покласти на директора Департаменту нотаріату, банкрутства та функціонування центрального засвідчувального органу Чижмарь К.І.

6. Цей наказ набирає чинності з дня його офіційного опублікування.

Міністр **О.В. Лавринович**

З оригіналом згідно

КОПІЯ

ЗАТВЕРДЖЕНО
Наказ Міністерства
юстиції України
29 січня 2010 року № 183/5

Регламент роботи центрального засвідчувального органу

I. Загальні положення

1.1. Цей Регламент розроблений відповідно до Закону України «Про електронний цифровий підпис», Положення про центральний засвідчувальний орган, затвердженого постановою Кабінету Міністрів України від 28 жовтня 2004 року № 1451, Правил посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3, зареєстрованих у Міністерстві юстиції України 27 січня 2005 року за № 104/10384, інших нормативно-правових актів, що регулюють відносини у сфері використання електронного цифрового підпису.

Цей Регламент визначає організаційно-методологічні та технологічні умови діяльності центрального засвідчувального органу (далі – ЦЗО) під час обслуговування посилених сертифікатів відкритих ключів (далі – сертифікати ключів) засвідчувальних центрів органів виконавчої влади або інших державних органів (далі – ЗЦ), центрів сертифікації ключів (далі – ЦСК) акредитованих центрів сертифікації ключів (далі – АЦСК) (далі разом – Центри), реєстрації, акредитації ЗЦ та ЦСК.

Цей Регламент є обов'язковим для суб'єктів правових відносин у сфері послуг електронного цифрового підпису (далі – ЕЦП) під час обслуговування ЦЗО сертифікатів ключів Центрів та проведення реєстрації, акредитації ЗЦ та ЦСК.

1.2. У цьому Регламенті терміни вживаються в таких значеннях:

заявник – юридична особа незалежно від форми власності або фізична особа, яка є суб'єктом підприємницької діяльності, що звертається до ЦЗО з метою проведення реєстрації ЗЦ або ЦСК;

локальна обчислювальна мережа – мережа передачі даних, що зв'язує декілька робочих станцій в одній локальній зоні, обмеженій приміщеннями адміністратора інформаційно-телекомунікаційної системи (далі – ІТС) ЦЗО (далі – Адміністратор ІТС ЦЗО).

Інші терміни, що вживаються у цьому Регламенті, застосовуються у значеннях, визначених нормативно-правовими актами, що регулюють відносини, які виникають у сфері ЕЦП.

1.3. Міністерство юстиції України відповідно до Положення про центральний засвідчувальний орган, затвердженого постановою Кабінету Міністрів України від 28 жовтня 2004 року № 1451, виконує такі функції ЦЗО:

здійснює реєстрацію, акредитацію ЗЦ та ЦСК, переакредитацію АЦСК, видачу, переоформлення та анулювання відповідних свідоцтв;

надає Центрам консультації з питань, пов'язаних з використанням ЕЦП;

забезпечує діяльність постійно діючої комісії з акредитації ЗЦ та ЦСК;

розглядає заяви і скарги щодо неналежного функціонування Центрів та подає відповідні пропозиції контролюючому органу;

повідомляє контролюючий орган про обставини, які перешкоджають діяльності ЦЗО;

здійснює інші функції, передбачені законодавством у сфері ЕЦП.

1.4. Технічне та технологічне забезпечення виконання функцій ЦЗО здійснюється Адміністратором ІТС ЦЗО.

Функції Адміністратора ІТС ЦЗО визначаються Міністерством юстиції України (далі – Мін'юст України).

Адміністратор ІТС ЦЗО забезпечує функціонування ІТС ЦЗО – організаційно-технологічної системи, що забезпечує обслуговування сертифікатів Центрів, та об'єднує програмно-технічний комплекс, фізичне середовище, обслуговуючий персонал, а також інформацію, що нею обробляється.

За допомогою ІТС ЦЗО Адміністратором ІТС ЦЗО забезпечуються:

генерація пари ключів (особистий та відкритий ключі) ЦЗО;

формування посилених сертифікатів власних відкритих ключів ЦЗО (далі – сертифікати ключів ЦЗО);

формування та видача сертифікатів ключів Центрів;

блокування, скасування, поновлення сертифікатів ключів Центрів;

ведення електронних реєстрів чинних, блокованих та скасованих сертифікатів ключів Центрів та їх розповсюдження (публікація);

зберігання сертифікатів ключів Центрів;

ведення Реєстру суб'єктів, які надають послуги, пов'язані з ЕЦП (далі – Реєстр суб'єктів);

функціонування офіційного веб-сайту ЦЗО;

формування та розповсюдження (публікація) списків відкликаних (скасованих, блокованих) сертифікатів ключів Центрів (далі – СВС), що формуються за допомогою відповідного електронного реєстру;

забезпечення цілодобового доступу до сертифікатів ключів ЦЗО, сертифікатів ключів Центрів, СВС та можливість перевірки статусу сертифікатів ключів Центрів у режимі реального часу через загальнодоступні телекомунікаційні мережі.

1.5. Формати, структура та протоколи, що застосовуються під час формування сертифікатів ключів ЦЗО, формування сертифікатів ключів Центрів, формування СВС Центрів, повинні відповідати вимогам наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 серпня 2012 року № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису», зареєстрованого в Міністерстві юстиції України 20 серпня 2012 року за № 1398/21710 (далі – Наказ).

1.6. Запит на формування сертифіката ключа Центру в електронному вигляді містить обов'язкові реквізити Центру, наведені в таблиці 1 додатка 1 до цього Регламенту.

1.7. Повне найменування державного органу, що виконує функції ЦЗО: Міністерство юстиції України. Скорочене найменування: Мін'юст України.

Місцезнаходження (поштова адреса): вул. Городецького, 13, м. Київ, 01001.

Код за ЄДРПОУ: 00015622.

Телефон: (044) 486-87-24; факс: (044) 486-87-24.

Адреса електронного інформаційного ресурсу ЦЗО, доступ до якого забезпечується через телекомунікаційні мережі загального користування

цілодобово (далі – офіційний веб-сайт ЦЗО): www.czo.gov.ua.

Електронна пошта ЦЗО: contact@czo.gov.ua.

1.8. Повне найменування підприємства, що здійснює функції Адміністратора ІТС ЦЗО: державне підприємство «Інформаційний центр» Міністерства юстиції України. Скорочене найменування: Держінформ'юст.

Місцезнаходження (поштова адреса): вул. Мельникова, 81, літ. А, м. Київ, 04050.

Код за ЄДРПОУ: 25287988.

Телефон: (044) 206-71-90; факс: (044) 206-71-28.

Електронна пошта: czo_admin_its@informjust.ua.

1.9. Діяльність Мін'юсту України та Адміністратора ІТС ЦЗО по роботі з Центрами щодо прийому заяв на реєстрацію, акредитацію ЗЦ та ЦСК, формування сертифікатів ключів Центрів, надання консультацій тощо організована в одну робочу зміну з понеділка по четвер з 9:00 до 18:00, обідня перерва – з 13:00 до 13:45; у п'ятницю – з 9:00 до 16:45, обідня перерва – з 13:00 до 13:45.

Діяльність Адміністратора ІТС ЦЗО по роботі з Центрами (заявниками) щодо блокування, скасування та поновлення сертифікатів ключів Центрів є цілодобовою. Інформування про необхідність подання до Адміністратора ІТС ЦЗО заяв на блокування, скасування та поновлення сертифікатів ключів Центрів у неробочий час здійснюється за телефоном (044) 206-71-90, а їх подання здійснюється за місцезнаходженням Адміністратора ІТС ЦЗО.

1.10. Заяви та документи на реєстрацію, акредитацію ЗЦ та ЦСК та формування сертифікатів ключів Центрам, документована інформація, що передається ЦЗО АЦСК у разі припинення їх діяльності, приймаються та розглядаються у робочі дні відповідно до режиму роботи, зазначеного в пункті 1.9 цього розділу.

1.11. Цей Регламент та зміни до нього розміщуються на офіційному веб-сайті ЦЗО.

1.12. Внесення змін та доповнень до Регламенту здійснюється ЦЗО у порядку, встановленому для погодження та затвердження Регламенту.

II. Сертифікати ключів, сформовані ЦЗО, та сфера їх використання

2.1. Адміністратор ІТС ЦЗО формує сертифікати ключів ЦЗО, що містять відкриті ключі, відповідні яким особисті ключі ЦЗО призначені для формування сертифікатів ключів Центрів, даних про статус

сертифікатів ключів Центрів та інших призначень, встановлених законодавством.

Сертифікати ключів ЦЗО використовуються для перевірки ЕЦП на сертифікатах ключів Центрів та на даних про статус сертифікатів ключів Центрів та інших призначень, встановлених законодавством.

2.2. Адміністратор ІТС ЦЗО формує сертифікати ключів Центрів, що містять відкриті ключі, відповідні яким особисті ключі Центрів призначені для формування сертифікатів ключів підписувачів, СВС та інших призначень, передбачених законодавством.

Сертифікати ключів Центрів використовуються для перевірки ЕЦП на сертифікатах ключів підписувачів та на СВС та для інших призначень, передбачених законодавством.

ІІІ. Інформація ЦЗО та порядок її розповсюдження (публікації)

3.1. На офіційному веб-сайті ЦЗО розповсюджується (публікується) така інформація:

перелік зареєстрованих ЗЦ та ЦСК;

перелік акредитованих ЗЦ та ЦСК;

сертифікати ключів ЦЗО;

електронні реєстри чинних, блокованих та скасованих сертифікатів ключів Центрів;

перелік Центрів, що припинили діяльність;

відомості про прийняття від АЦСК на зберігання документованої інформації у разі припинення діяльності АЦСК;

нормативно-правові акти, що регулюють відносини у сфері використання ЕЦП, Регламент, фотокопії свідоцтв про акредитацію, зразок договору про надання послуг з обслуговування посилених сертифікатів відкритих ключів Центру та інших документів, методичні та довідкові матеріали;

інформація щодо поточної діяльності ЦЗО.

3.2. Публікація чинних сертифікатів ключів ЦЗО здійснюється після формування сертифікатів.

Публікація чинних сертифікатів ключів Центрів здійснюється після передачі сформованого сертифіката уповноваженій особі Центру.

Доступ до сертифікатів ЦЗО та Центрів забезпечується цілодобово.

3.3. Інформація щодо скасованих та блокованих сертифікатів Центрів публікується на офіційному веб-сайті ЦЗО у вигляді повних та

часткових СВС, формати яких встановлені Вимогами до формату посиленого сертифіката відкритого ключа, затвердженими Наказом.

Повні СВС публікуються не рідше одного разу на тиждень не пізніше закінчення строку дії попереднього СВС.

Часткові СВС публікуються не рідше одного разу на дві години не пізніше закінчення строку дії попереднього СВС.

Доступ до СВС забезпечується цілодобово.

IV. Порядок ідентифікації та автентифікації Центрів, реєстрації ЗЦ та ЦСК, акредитації ЗЦ та ЦСК

1. Загальні положення

1.1. Ідентифікація та автентифікація заявників здійснюються в процесі проведення процедур реєстрації та акредитації Центрів, формування, повторного формування сертифіката ключа Центру, блокування, скасування, поновлення сертифіката ключа Центру.

1.2. Перед проведенням реєстрації, акредитації, формуванням сертифіката ключа Центру або наданням послуг з обслуговування сертифікатів ключів виконується процедура встановлення заявника або його уповноваженої особи (ідентифікація та автентифікація).

Встановлення юридичної особи здійснюється за її установчими документами, відомостями з Єдиного державного реєстру юридичних осіб та фізичних осіб – підприємців. Встановлення фізичної особи здійснюється за паспортом або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи (паспорт громадянина України, паспорт громадянина України для виїзду за кордон, дипломатичний чи службовий паспорт, посвідчення особи моряка, посвідка на проживання особи, яка мешкає в Україні, національний паспорт іноземця або документ, що його замінює).

Встановлення повноважень особи здійснюється за документом, що підтверджує її повноваження.

2. Реєстрація ЗЦ або ЦСК

2.1. Реєстрація ЗЦ або ЦСК відбувається шляхом внесення інформації про ЗЦ або ЦСК до Реєстру суб'єктів.

2.2. Реєстрація ЗЦ або ЦСК здійснюється на підставі заяви на проведення реєстрації за формою, визначеною у додатку 2 до цього Регламенту (далі – заява форми 1), що подається до Мін'юсту України в письмовій формі заявником або його уповноваженою особою і підписується керівником заявника та скріплюється печаткою.

2.3. У заяві форми 1 зазначаються:

повне найменування юридичної особи, посада, прізвище, ім'я та по батькові її керівника (прізвище, ім'я та по батькові фізичної особи, яка є суб'єктом підприємницької діяльності, серія і номер паспорта, ким і коли виданий);

організаційно-правова форма;

код згідно з ЄДРПОУ (для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки платника податків з Державного реєстру фізичних осіб – платників податків);

номер поточного рахунку та найменування банку;

місце реєстрації юридичної особи (фізичної особи – суб'єкта підприємницької діяльності);

номери телефонів;

електронна адреса інформаційного ресурсу;

адреса електронної пошти;

назва ЦСК, ЗЦ;

відомості про контактну особу (прізвище, ім'я та по батькові, посада, номери телефонів, адреса електронної пошти).

2.4. Разом із заявою форми 1 заявник – юридична особа подає такі документи:

копії установчих документів, засвідчені в установленому порядку;

виписку або витяг з Єдиного державного реєстру юридичних осіб та фізичних осіб-підприємців;

копію документа, що підтверджує право власності заявника на окреме приміщення або оренди такого приміщення, засвідчену в установленому порядку;

список посадових осіб заявника та засвідчені в установленому порядку копії документів про рівень освіти і кваліфікації керівника ЗЦ або ЦСК та посадових осіб, обов'язки яких безпосередньо пов'язані з наданням послуг ЕЦП та обслуговуванням сертифікатів ключів;

положення, яким визначаються посадові обов'язки, кваліфікаційні вимоги посадових осіб заявника.

До заяви форми 1 заявник – фізична особа, яка є суб'єктом підприємницької діяльності, додає такі документи:

виписку або витяг з Єдиного державного реєстру юридичних осіб та фізичних осіб – підприємців;

паспорт та його копію, засвідчену в установленому порядку;

копію документа, що підтверджує право власності заявника на окреме приміщення або оренди такого приміщення, засвідчену в установленому порядку;

список посадових осіб заявника та засвідчені в установленому порядку копії документів про рівень освіти і кваліфікації керівника ЗЦ або ЦСК та посадових осіб, обов'язки яких безпосередньо пов'язані з наданням послуг ЕЦП та обслуговуванням сертифікатів ключів;

положення, яким визначаються посадові обов'язки, кваліфікаційні вимоги посадових осіб заявника.

2.5. Опрацювання заяви форми 1 здійснюється у разі наявності всіх документів відповідно до переліку, визначеного пунктом 2.4 цієї глави.

Не приймаються до розгляду заяви та документи, що мають підчистки, дописки, закреслені слова, інші незастережені виправлення або написи олівцем, а також пошкодження, внаслідок чого їхній текст не можна прочитати.

2.6. Розгляд заяви на реєстрацію становить не більше п'яти робочих днів від дати прийняття заяви.

2.7. Рішення про реєстрацію ЗЦ або ЦСК приймається у вигляді наказу Мін'юсту України за умови відповідності документів, поданих разом із заявою, вимогам, встановленим цим Регламентом. В іншому випадку надається мотивована відмова у проведенні реєстрації.

У разі прийняття рішення про реєстрацію ЗЦ або ЦСК для внесення відповідної інформації про ЗЦ та ЦСК до Реєстру суб'єктів Мін'юст України надсилає до Адміністратора ІТС ЦЗО такі документи:

копію заяви форми 1, поданої заявником;

копії документів, поданих разом із заявою форми 1;

копію рішення про реєстрацію.

У разі прийняття рішення про реєстрацію ЗЦ або ЦСК засвідчують свій відкритий ключ у ЦЗО відповідно до вимог Регламенту.

3. Акредитація ЗЦ та ЦСК

3.1. Проведення акредитації ЗЦ та ЦСК здійснюється у строк та відповідно до Порядку акредитації центру сертифікації ключів, затвердженого постановою Кабінету Міністрів України від 13 липня 2004 року № 903.

3.2. Акредитація ЗЦ та ЦСК проводиться на підставі заяви на проведення акредитації за формою, визначеною у додатку 3 до цього Регламенту (далі – заява форми 2), що подається до Мін'юсту України.

3.3. У заяві форми 2 зазначаються:

повне найменування юридичної особи, посада, прізвище, ім'я та по батькові її керівника (прізвище, ім'я та по батькові фізичної особи, яка є суб'єктом підприємницької діяльності, серія і номер паспорта, ким і коли виданий);

організаційно-правова форма;

код згідно з ЄДРПОУ (для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки платника податків з Державного реєстру фізичних осіб – платників податків);

номер поточного рахунку та найменування банку;

місце реєстрації юридичної особи (фізичної особи – суб'єкта підприємницької діяльності);

номери телефонів;

електронна адреса інформаційного ресурсу;

адреса електронної пошти;

назва ЦСК, ЗЦ;

відомості про контактну особу (прізвище, ім'я та по батькові, посада, номери телефонів, адреса електронної пошти).

3.4. Разом із заявою форми 2 ЗЦ та ЦСК подають документи згідно з переліком, визначеним у додатку 1 до Порядку акредитації центру сертифікації ключів, затвердженого постановою Кабінету Міністрів України від 13 липня 2004 року № 903.

3.5. Не приймаються до розгляду заяви та документи, які мають підчистки, дописки, закреслені слова, інші незастережені виправлення або написи олівцем, а також пошкодження, внаслідок чого їхній текст не можна прочитати.

3.6. Рішення про акредитацію ЗЦ або ЦСК приймається у вигляді наказу Мін'юсту України.

У разі прийняття рішення про акредитацію для внесення відповідної інформації про АЦСК до Реєстру суб'єктів відповідний структурний підрозділ Мін'юсту України надсилає до Адміністратора ІТС ЦЗО такі документи:

копію заяви форми 2, поданої заявником;

копії документів, поданих разом із заявою форми 2;

копію рішення про акредитацію.

У разі прийняття рішення про акредитацію ЗЦ або ЦСК засвідчує свій відкритий ключ у ЦЗО відповідно до вимог цього Регламенту.

V. Обслуговування сертифікатів ключів Центрів

1. Формування сертифікатів ключів Центру

1.1. Формування сертифіката ключа Центру здійснюється на підставі заяви на формування посиленого сертифіката відкритого ключа за формою, визначеною у додатку 4 до цього Регламенту (далі – заява форми 3), що подається до Адміністратора ІТС ЦЗО.

1.2. Заява форми 3 подається до Адміністратора ІТС ЦЗО в письмовій формі особисто керівником юридичної особи – Центру (фізичною особою, яка є суб'єктом підприємницької діяльності, що є Центром) або його уповноваженою особою, підписується ним або його уповноваженою особою та скріплюється печаткою.

Під час прийому заяви форми 3 здійснюється встановлення особи керівника юридичної особи – Центру (фізичної особи, яка є суб'єктом підприємницької діяльності, що є Центром) або його уповноваженої особи.

1.3. У заяві форми 3 зазначаються:

повне найменування юридичної особи, посада, прізвище, ім'я та по батькові її керівника (прізвище, ім'я та по батькові фізичної особи, яка є суб'єктом підприємницької діяльності, серія і номер паспорта, ким і коли виданий);

організаційно-правова форма;

код згідно з ЄДРПОУ (для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки платника податків з Державного реєстру фізичних осіб – платників податків);

місце реєстрації юридичної особи (фізичної особи – суб'єкта підприємницької діяльності);

номери телефонів;

електронна адреса інформаційного ресурсу;

адреса електронної пошти;

назва Центру;

серійний (заводський) номер носія інформації, на якому надається запит на формування сертифіката в електронному вигляді;

унікальний реєстраційний номер, що входить до реквізиту «унікальний реєстраційний номер» (поле "SerialNumber") сертифіката ключа Центру;

призначення (сфера використання) відкритого ключа Центру відповідно до вимог, встановлених законодавством.

Не приймаються до розгляду заяви та документи, що мають підчистки, дописки, закреслені слова, інші незастережені виправлення або написи олівцем, а також пошкодження, внаслідок чого їхній текст не можна прочитати.

1.4. Формування Центром унікального реєстраційного номера, що входить до реквізиту «унікальний реєстраційний номер» сертифіката ключа Центру, здійснюється згідно з нижченаведеними правилами:

UA-[КодУстанови] {-[Додаток]},

де

UA – код України згідно з ISO 3166;

КодУстанови – 8, 9 або 10 цифр, що містять код згідно з ЄДРПОУ організації – юридичної особи (для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки платника податків з Державного реєстру фізичних осіб – платників податків), що є Центром, за відомостями установчих документів та/або відомостями з Єдиного державного реєстру юридичних осіб та фізичних осіб – підприємців;

додаток – необов'язкова послідовність від 1 до 4 цифр, що містить додаткову частину ідентифікатора. У разі використання додатка він відокремлюється від реквізиту КодУстанови символом "–".

Вищезазначений реквізит шляхом його додавання до розпізнавального імені Центру забезпечує унікальність його розпізнавального імені в межах України.

1.5. Разом із заявою форми 3 подаються:

запит на формування сертифіката ключа Центру (далі – запит) в електронному вигляді;

два примірники договору про надання послуг з обслуговування посиленого сертифіката відкритого ключа, підписані керівником юридичної особи – Центру (фізичною особою, яка є суб'єктом підприємницької діяльності, що є Центром) або його уповноваженою особою та скріплені печаткою.

1.6. Вимоги до запиту:

запит подається у форматі згідно зі специфікацією синтаксису запиту на сертифікацію (PKCS#10), що визначена RFC 2986 "PKCS #10: Certification Request Syntax Specification";

запит повинен містити інформацію про відкритий ключ Центру, що подає такий запит. Зазначена інформація визначається атрибутом «Інформація про відкритий ключ підписувача» («subjectPublicKeyInfo»), формат якого повинен відповідати Вимогам до формату посиленого сертифіката відкритого ключа, затвердженим Наказом;

формат інших обов'язкових полів запиту повинен відповідати вимогам Наказу;

запит, крім обов'язкових реквізитів Центру, може містити додаткову інформацію відносно Центру, що подає такий запит. Зазначена інформація визначається атрибутом «Розширений запит» («extensionRequest»);

атрибут «Розширений запит» використовується для визначення розширень у сертифікаті ключа Центру, що формується, та має такий вигляд:

```
extensionRequest ATTRIBUTE ::= {
        WITH SYNTAX ExtensionRequest
        SINGLE VALUE TRUE
        ID pkcs-9-at-extensionRequest
}
ExtensionRequest ::= Extensions
```

формат поля Extensions повинен відповідати Вимогам до формату посиленого сертифіката відкритого ключа, затвердженим Наказом.

1.7. Розгляд заяви форми 3 становить не більше двох робочих днів від дати прийняття заяви.

Під час розгляду заяви форми 3 здійснюється перевірка:

відповідності даних, внесених до заяви, документам Центру, отриманим від Мін'юсту України відповідно до пункту 2.7 глави 2 та пункту 3.6 глави 3 розділу IV цього Регламенту;

унікальності розпізнавального імені Центру в межах України;

унікальності відкритого ключа Центру за відомостями реєстру чинних, блокованих та скасованих сертифікатів ключів Центрів;

належності Центру відповідного особистого ключа шляхом перевірки ЕЦП на запиті на формування сертифіката ключа Центру;

відповідності запиту на формування сертифіката вимогам, зазначеним у пункті 1.6 цієї глави.

У разі успішної перевірки Адміністратор ІТС ЦЗО формує сертифікат ключа Центру. У разі непроходження перевірки Центру надається мотивована відмова у формуванні сертифіката Центру та повертається заява форми 3 разом з додатками до неї.

1.8. Формування сертифікатів ключів Центрів здійснюється посадовими особами Адміністратора ІТС ЦЗО, на яких покладено виконання обов'язків адміністратора сертифікації (далі – адміністратор сертифікації), та під контролем посадових осіб Адміністратора ІТС ЦЗО,

на яких покладено виконання обов'язків адміністратора безпеки (далі – адміністратор безпеки).

Під час формування сертифіката ключа Центру:

розширення, подані у запиті, обробляються за правилами, наведеними в таблиці 2 додатка 1 до цього Регламенту;

додаткові розширення, що не наведені в таблиці 2 додатка 1 до цього Регламенту та можуть міститись у запиті, встановлюються у сертифікаті ключа Центру за умови, що вони були визначені як некритичні, а об'єктні ідентифікатори таких розширень зареєстровані у встановленому порядку.

Адміністратор ІТС ЦЗО формує сертифікат ключа Центру в електронній формі та два примірники сертифіката ключа Центру в паперовій формі.

Усі примірники сертифіката ключа Центру у паперовій формі підписуються керівником юридичної особи – Центру (фізичною особою, яка є суб'єктом підприємницької діяльності, що є Центром) або його уповноваженою особою, уповноваженою особою Адміністратора ІТС ЦЗО та скріплюються печаткою Адміністратора ІТС ЦЗО.

1.9. За результатами проведеного формування сертифіката ключа Центру його уповноваженій особі надаються:

один підписаний примірник договору про надання Центру Адміністратором ІТС ЦЗО послуг з обслуговування посиленого сертифіката відкритого ключа;

один примірник сертифіката ключа Центру в паперовій формі;

сертифікат ключа Центру в електронній формі;

сертифікати ключів ЦЗО в електронній формі.

Дані в електронній формі передаються уповноваженій особі Центру у вигляді файлів, записаних на оптичний диск або інший носій.

1.10. Строк чинності сертифіката ключа Центру визначається відповідно до вимог законодавства про ЕЦП.

Початок строку чинності сертифіката ключа Центру обчислюється з дати і часу формування сертифіката у ЦЗО, що відображається у сертифікаті.

1.11. Після передачі сертифіката ключа Центру відповідно до пункту 1.9 цієї глави сертифікат ключа опубліковується на офіційному веб-сайті ЦЗО.

1.12. Центри використовують пари (особистих та відкритих) ключів зі ступенем розширення основного поля еліптичної кривої згідно з

ДСТУ 4145-2002 «Інформаційна технологія. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих», затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі – ДСТУ 4145-2002), не менше 257.

Центр використовує особистий ключ Центру тільки за призначенням (сферою використання) в період чинності сертифіката ключа Центру та за умови, що сертифікат ключа Центру не був заблокований або скасований.

Центр забезпечує використання сертифіката ключа Центру та особистого ключа Центру тільки в рамках сфери використання, зазначеної у пункті 2.2 розділу ІІ цього Регламенту.

Центр забезпечує обов'язковість перевірки строку чинності та статусу сформованого ЦЗО сертифіката ключа Центру під час надання послуг ЕЦП у порядку, встановленому законодавством.

Перед використанням сертифіката ключа Центру здійснюються:

перевірка чинності сертифіката ключа Центру на момент накладення ЕЦП на документ або перевірка ЕЦП на документі;

перевірка ЕЦП сертифіката ключа Центру за допомогою сертифіката ключа ЦЗО, чинного на момент формування сертифіката ключа Центру;

перевірка статусу сертифіката ключа Центру у режимі реального часу, якщо перевірка здійснюється на момент чинності сертифіката Центру, або за СВС.

Під час перевірки статусу сертифіката ключа Центру за СВС здійснюється перевірка автентичності, цілісності та терміну дії СВС.

2. Скасування сертифіката ключа Центру

2.1. Скасування сертифіката ключа Центру здійснюється у випадках, передбачених законодавством, на підставі заяви на скасування посиленого сертифіката відкритого ключа за формою, визначеною у додатку 5 до цього Регламенту (далі – заява форми 4), що подається до Адміністратора ІТС ЦЗО.

2.2. Заява форми 4 подається до Адміністратора ІТС ЦЗО в письмовій формі особисто керівником юридичної особи – Центру (фізичною особою, яка є суб'єктом підприємницької діяльності, що є Центром) або його уповноваженою особою, підписується ним або його уповноваженою особою та скріплюється печаткою.

Під час прийому заяви форми 4 здійснюється встановлення особи керівника юридичної особи – Центру (фізичної особи, яка є суб'єктом підприємницької діяльності, що є Центром) або його уповноваженої особи.

2.3. У заяві форми 4 зазначаються:

повне найменування юридичної особи, посада, прізвище, ім'я та по батькові її керівника (прізвище, ім'я та по батькові фізичної особи, яка є суб'єктом підприємницької діяльності, серія і номер паспорта, ким і коли виданий);

код згідно з ЄДРПОУ (для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки платника податків з Державного реєстру фізичних осіб – платників податків);

номери телефонів;

електронна адреса електронного інформаційного ресурсу;

причина скасування сертифіката ключа Центру;

назва Центру;

унікальний реєстраційний номер сертифіката ключа Центру, що скасовується.

Не приймається до розгляду заява, що має підчистки, дописки, закреслені слова, інші незастережені виправлення або написи олівцем, а також пошкодження, внаслідок чого її текст не можна прочитати.

2.4. Опрацювання заяви форми 4 та інформування Центром Адміністратора ЦЗО про скасування сертифіката його ключа здійснюються протягом двох годин від моменту отримання заяви Адміністратором ІТС ЦЗО.

Скасування сертифікатів ключів Центрів здійснюється адміністратором сертифікації під контролем адміністратора безпеки.

Скасування сертифіката ключа Центру набирає чинності з моменту внесення відомостей про нього до електронних реєстрів чинних, блокованих та скасованих сертифікатів ключів Центрів із зазначенням причини, дати та часу здійснення цієї операції.

3. Блокування сертифіката ключа Центру

3.1. Блокування сертифіката ключа Центру здійснюється у випадках, передбачених законом, на підставі заяви на блокування посиленого сертифіката відкритого ключа за формою, визначеною у додатку 6 до цього Регламенту (далі – заява форми 5), що подається до Адміністратора ІТС ЦЗО.

3.2. Заява форми 5 подається до Адміністратора ІТС ЦЗО в письмовій формі особисто керівником юридичної особи – Центру (фізичною особою, яка є суб'єктом підприємницької діяльності, що є Центром) або його уповноваженою особою, підписується ним або його уповноваженою особою та скріплюється печаткою.

Під час прийому заяви форми 5 здійснюється встановлення особи керівника юридичної особи – Центру (фізичної особи, яка є суб'єктом підприємницької діяльності, що є Центром) або його уповноваженої особи.

3.3. У заяві форми 5 зазначаються:

повне найменування юридичної особи, посада, прізвище, ім'я та по батькові її керівника (прізвище, ім'я та по батькові фізичної особи, яка є суб'єктом підприємницької діяльності, серія і номер паспорта, ким і коли виданий);

код згідно з ЄДРПОУ (для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки платника податків з Державного реєстру фізичних осіб – платників податків);

номери телефонів;

електронна адреса інформаційного ресурсу;

адреса електронної пошти;

причина блокування сертифіката ключа Центру;

назва Центру;

унікальний реєстраційний номер сертифіката ключа Центру, що блокується.

Не приймається до розгляду заява, що має підчистки, дописки, закреслені слова, інші незастережені виправлення або написи олівцем, а також пошкодження, внаслідок чого її текст не можна прочитати.

3.4. Опрацювання заяви форми 5 та інформування Центром Адміністратора ЦЗО про блокування сертифіката його ключа здійснюються протягом двох годин від моменту отримання заяви Адміністратором ІТС ЦЗО.

Блокування сертифіката ключа Центру здійснюється адміністратором сертифікації під контролем адміністратора безпеки.

Блокування сертифіката ключа Центру набирає чинності з моменту внесення відомостей про нього до електронних реєстрів чинних, блокованих та скасованих сертифікатів ключів Центрів із зазначенням причини, дати та часу здійснення цієї операції.

4. Поновлення сертифіката ключа Центру

4.1. Поновлення сертифіката ключа Центру здійснюється у випадках, передбачених законодавством, на підставі заяви на поновлення посиленого сертифіката відкритого ключа за формою, визначеною у додатку 7 до цього Регламенту (далі – заява форми 6), що подається до Адміністратора ІТС ЦЗО.

4.2. Заява форми 6 подається до Адміністратора ІТС ЦЗО в письмовій формі особисто керівником юридичної особи – Центру (фізичною особою, яка є суб'єктом підприємницької діяльності, що є Центром) або його уповноваженою особою, підписується ним або його уповноваженою особою та скріплюється печаткою.

Під час прийому заяви форми 6 здійснюється встановлення особи керівника юридичної особи – Центру (фізичної особи, яка є суб'єктом підприємницької діяльності, що є Центром) або його уповноваженої особи.

4.3. У заяві форми 6 зазначаються:

повне найменування юридичної особи, посада, прізвище, ім'я та по батькові її керівника (прізвище, ім'я та по батькові фізичної особи, яка є суб'єктом підприємницької діяльності, серія і номер паспорта, ким і коли виданий);

код згідно з ЄДРПОУ (для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки платника податків з Державного реєстру фізичних осіб – платників податків);

номери телефонів;

електронна адреса інформаційного ресурсу;

адреса електронної пошти;

причина поновлення сертифіката ключа;

назва Центру;

унікальний реєстраційний номер сертифіката ключа Центру, що поновлюється.

Не приймається до розгляду заява, що має підчистки, дописки, закреслені слова, інші незастережені виправлення або написи олівцем, а також пошкодження, внаслідок чого її текст не можна прочитати.

4.4. Опрацювання заяви форми 6 здійснюється протягом двох годин від моменту отримання заяви Адміністратором ІТС ЦЗО.

4.5. Поновлення сертифіката ключа Центру здійснюється адміністратором сертифікації під контролем адміністратора безпеки.

Поновлення сертифіката ключа Центру набирає чинності з моменту внесення відомостей про нього до електронних реєстрів чинних, блокованих та скасованих сертифікатів ключів Центрів із зазначенням причини, дати та часу здійснення цієї операції.

Скасований сертифікат ключа Центру не може бути поновлений.

4.6. Розповсюдження інформації про статус сертифікатів ключів Центрів здійснюється за допомогою публікації повного та часткового

СВС на офіційному веб-сайті ЦЗО та забезпечення можливості перевірки статусу сертифіката ключа Центру в режимі реального часу через телекомунікаційні мережі загального користування.

Адміністратор ІТС ЦЗО під час формування СВС забезпечує такі умови:

кожен із СВС містить дані щодо часу видання наступного списку;

новий СВС може бути опублікований до визначеного часу видання наступного списку;

на СВС накладається ЕЦП з використанням особистого ключа ЦЗО.

Інформація про статус сертифіката ключа Центру в режимі реального часу розповсюджується за протоколом визначення статусу сертифіката згідно з Вимогами до протоколу визначення статусу сертифіката, затвердженими Наказом.

Публікація наступного СВС здійснюється з періодичністю, зазначеною у пункті 3.3 розділу ІІІ цього Регламенту.

VI. Управління та операційний контроль

1. Фізичне середовище

1.1. Приміщення, де розташовано ІТС ЦЗО, територіально поділене на дві частини, в яких розміщено локальні обчислювальні мережі (далі – ЛОМ) управління ІТС ЦЗО та ЛОМ серверів ІТС ЦЗО.

Місцезнаходження ЛОМ управління ІТС ЦЗО: вул. Мельникова, 81, літ. А, м. Київ, 04050.

Місцезнаходження ЛОМ серверів ІТС ЦЗО: вул. Ливарська, 1, літ. А, м. Київ, 04073.

1.2. У ЛОМ управління об'єднані робочі станції (далі – РС) посадових осіб Адміністратора ІТС ЦЗО, на яких покладено виконання обов'язків адміністратора реєстрації (далі – адміністратор реєстрації), посадових осіб Адміністратора ІТС ЦЗО, на яких покладено виконання обов'язків системного адміністратора (далі – системний адміністратор), адміністраторів сертифікації та безпеки (далі разом – адміністратори) з використанням комутаційного обладнання та які розміщуються відокремлено від серверів і підключаються до ЛОМ серверів ІТС ЦЗО через телекомунікаційні мережі загального користування. Підключення здійснюється через шлюз захисту мережевих з'єднань, який розміщується на стороні ЛОМ серверів ІТС ЦЗО таким чином, що утворюється єдина віртуальна ЛОМ система. Шлюз захисту мережевих з'єднань призначений для автентифікації адміністраторів при підключенні до ЛОМ серверів шляхом встановлення захищеного мережевого з'єднання з РС адміністраторів.

1.3. Приміщення, де розміщено ЛОМ серверів ІТС ЦЗО, обладнано згідно з вимогами до спеціальних приміщень АЦСК, які передбачають проведення заходів щодо пасивного захисту інформації від її витоку каналами побічних електромагнітних випромінювань та наведень, а також від порушення її цілісності внаслідок деструктивного впливу зовнішніх електромагнітних полів (далі – спеціальне приміщення).

Усі приміщення ІТС ЦЗО обладнані автоматичною системою контролю доступу, яка забезпечує фізичний доступ до приміщень тільки особам, визначеним наказом керівника Адміністратора ІТС ЦЗО.

2. Безпека ІТС ЦЗО та захист інформаційних ресурсів

2.1. Для виконання технічних та технологічних функцій ЦЗО Адміністратором ІТС ЦЗО створюється технічний підрозділ, до складу якого входять працівники, діяльність яких безпосередньо пов'язана із забезпеченням функціонування ІТС ЦЗО.

Захист інформації у ІТС ЦЗО забезпечується службою захисту інформації ІТС ЦЗО.

Безпека ІТС ЦЗО досягається шляхом впровадження організаційних інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації комплексної системи захисту інформації (далі – КСЗІ).

Засоби та обладнання ІТС ЦЗО, за допомогою яких здійснюються генерація та використання особистого ключа ЦЗО, обслуговування сертифікатів ключів Центрів, розміщуються у спеціальному приміщенні. Фізичний доступ до обладнання ІТС ЦЗО, що забезпечує генерацію та використання особистих ключів ЦЗО, сертифікацію, управління статусом сертифіката, обмежений і надається виключно посадовим особам Адміністратора ІТС ЦЗО, визначеним наказом керівника Адміністратора ІТС ЦЗО.

2.2. В ІТС ЦЗО забезпечується захист інформаційних ресурсів від зовнішніх загроз, атак та несанкціонованого витоку інформації шляхом створення та підтримки безпечних інформаційних технологій, у рамках яких доступ до інформації різних категорій користувачів організовується таким чином, що тільки уповноваженим користувачам або процесам надається можливість роботи з конкретною інформацією, доступ до якої обмежується і гарантується цілісність при її обробці в електронному вигляді набором даних, що містяться на змінних носіях інформації.

Робота ІТС ЦЗО можлива лише при функціонуючій КСЗІ.

У спеціальному приміщенні, де розташовано ЛОМ серверів ІТС ЦЗО, передбачено захист внутрішньої обчислювальної мережі від втручання з боку телекомунікаційної мережі загального користування.

Доступ до захищених ресурсів ІТС ЦЗО надається тільки після успішної авторизації адміністраторів.

Перед початком виконання процедур, пов'язаних із реєстрацією, формуванням сертифіката ключа або зміною його статусу, формуванням СВС, адміністратори повинні бути успішно авторизовані.

3. Процедурний контроль

3.1. У складі технічного підрозділу Адміністратора ІТС ЦЗО, який здійснює забезпечення функціонування ІТС ЦЗО, створюється служба захисту інформації у складі:

посадової особи Адміністратора ІТС ЦЗО, на яку покладено обов'язки керівника служби захисту інформації;

адміністратора безпеки;

системного адміністратора.

До складу технічного підрозділу Адміністратора ІТС ЦЗО також входять:

адміністратор сертифікації;

адміністратор реєстрації.

Служба захисту інформації ІТС ЦЗО (далі — СЗІ) забезпечує захист інформації в ІТС ЦЗО шляхом вирішення питань, пов'язаних з проектуванням, розробленням, модернізацією, введенням в експлуатацію та підтримкою працездатності КСЗІ, та додержання режиму безпеки в ІТС ЦЗО.

Основними функціями СЗІ є:

забезпечення повноти та якісного виконання організаційно-технічних заходів із захисту інформації;

розроблення розпорядчих документів, згідно з якими Адміністратор ІТС ЦЗО повинен забезпечувати захист інформації, контроль за їх виконанням;

своєчасне реагування на спроби несанкціонованого доступу до інформаційних ресурсів ІТС ЦЗО, порушення правил експлуатації засобів захисту інформації.

Обов'язки керівника СЗІ покладаються на одного із працівників технічного підрозділу Адміністратора ІТС ЦЗО наказом керівника Адміністратора ІТС ЦЗО.

Керівник СЗІ забезпечує належне виконання СЗІ її функцій.

3.2. Адміністратор безпеки відповідає за належне функціонування КСЗІ.

Основними обов'язками адміністратора безпеки є:

участь у генерації пари ключів (особистий та відкритий ключі) ЦЗО та їх резервних копій;

контроль за формуванням, резервуванням та обслуговуванням сертифікатів ключів ЦЗО, Центрів та СВС;

контроль за зберіганням особистих ключів ЦЗО та їх резервних копій, особистих ключів адміністраторів;

участь у знищенні особистих ключів ЦЗО, контроль за правильним і своєчасним знищенням адміністраторами особистих ключів;

організація розмежування доступу до ресурсів ІТС ЦЗО;

забезпечення спостереження (реєстрація та аудит подій у ІТС ЦЗО, моніторинг подій тощо) за функціонуванням КСЗІ;

забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій ІТС ЦЗО;

забезпечення режиму доступу до спеціального приміщення ІТС ЦЗО;

ведення журналів обліку адміністратора безпеки, передбачених документацією КСЗІ.

3.3. Системний адміністратор відповідає за функціонування ІТС ЦЗО.

Основними обов'язками системного адміністратора є:

організація експлуатації та технічного обслуговування ІТС ЦЗО і адміністрування його засобів;

забезпечення функціонування офіційного веб-сайту ЦЗО;

участь у впровадженні та забезпеченні функціонування КСЗІ;

ведення журналів аудиту подій, що реєструють засоби ІТС ЦЗО;

інсталяція та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення ІТС ЦЗО;

встановлення та налагодження штатної підсистеми резервного копіювання бази даних ІТС ЦЗО;

забезпечення актуалізації баз даних, створюваних та оброблюваних у ІТС ЦЗО, внаслідок збоїв.

3.4. Адміністратор сертифікації відповідає за формування сертифікатів ключів, ведення електронних реєстрів чинних, блокованих та скасованих сертифікатів ключів, збереження та використання особистого ключа ЦЗО.

Основними обов'язками адміністратора сертифікації є:

участь у генерації пари ключів (особистий та відкритий ключі) та зберігання особистих ключів ЦЗО та їх резервних копій;

забезпечення використання особистих ключів ЦЗО під час формування та обслуговування сертифікатів ключів ЦЗО та Центрів;

перевірка запитів на формування сертифікатів Центру вимогам Регламенту;

участь у знищенні особистих ключів ЦЗО;

забезпечення ведення, архівування та відновлення баз даних сертифікатів ключів Центрів;

розповсюдження (публікація) переліку сертифікатів ключів Центрів і СВС на офіційному веб-сайті ЦЗО;

резервування сертифікатів ключів і СВС, інших важливих ресурсів ІТС ЦЗО.

3.5. Адміністратор реєстрації відповідає за перевірку документів, наданих Центрами, звернень Центрів щодо формування, блокування, поновлення та скасування сертифікатів ключів Центрів.

Основними обов'язками адміністратора реєстрації є:

ідентифікація та автентифікація заявників;

перевірка заяв на формування, скасування, блокування та поновлення сертифікатів ключів;

встановлення належності Центру особистого ключа та його відповідності відкритому ключу Центру;

ведення електронного Реєстру суб'єктів.

4. Журнали аудиту

4.1. У журналах аудиту ІТС ЦЗО реєструються дії та події таких типів:

спроби створення, знищення, встановлення паролів, зміни прав доступу в ІТС ЦЗО тощо;

заміни технічних засобів ІТС ЦЗО та ключів;

формування, блокування, скасування та поновлення сертифікатів ключів, формування всіх СВС;

спроби несанкціонованого доступу до ІТС ЦЗО;

надання доступу персоналу до ІТС ЦЗО;

зміна системних конфігурацій та технічне обслуговування ІТС ЦЗО;

збої в роботі ІТС ЦЗО;

інші події, відомості про які фіксуються в журналі аудиту ІТС ЦЗО.

Усі записи в журналах аудиту в електронній або паперовій формі повинні містити дату та час дії або події, а також ідентифікувати суб'єкта, що її здійснив або ініціював.

4.2. Журнали аудиту підлягають перегляду не рідше одного разу на тиждень. Перегляд передбачає перевірку того, що журнал не піддавався несанкціонованим модифікаціям, вивчення всіх дій та/або подій у журналі з приділенням особливої уваги повідомленням про невідповідності і попередженням про небезпечні ситуації. Перегляд журналів аудиту ІТС ЦЗО здійснює адміністратор безпеки. Результати перегляду адміністратор безпеки фіксує в журналі аудиту адміністратора безпеки.

4.3. Система ведення електронного журналу аудиту включає механізми його захисту від неавторизованого перегляду, модифікації і знищення. Записи подій у журналах аудиту в паперовій формі повинні бути завірені і підписані адміністратором безпеки.

Журнали аудиту в електронній формі резервуються з періодичністю не менше одного разу на тиждень.

4.4. Адміністратор ІТС ЦЗО зберігає журнали аудиту на місці їх створення протягом 10 років, після чого забезпечує їх передачу для архівного збереження.

5. Ведення архівів

Документи з паперовими та електронними носіями, що створюються або надходять до ЦЗО, зберігаються та знищуються відповідно до вимог законодавства.

VII. Періодичність, порядок планової заміни, використання особистих ключів ЦЗО та управління ключами в ЦЗО

1. Загальні положення

В ІТС ЦЗО використовуються такі особисті та відповідні їм відкриті ключі:

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки ЕЦП на сертифікатах ключів ЦЗО, Центрів та СВС зі ступенем розширення основного поля еліптичної кривої не менше 431 згідно з ДСТУ 4145-2002;

особисті та відповідні їм відкриті ключі ЦЗО для накладення та перевірки ЕЦП на даних про статус сертифікатів ключів Центрів, що визначається в режимі реального часу, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;

особисті та відповідні їм відкриті ключі шлюзу захисту мережевих з'єднань зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;

особисті та відповідні їм відкриті ключі адміністраторів, що використовуються для криптографічного захисту мережевих з'єднань, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002.

Процедури генерації особистих та відповідних їм відкритих ключів, що використовуються в ІТС ЦЗО, створення резервних копій, відновлення із резервних копій, використання та знищення особистих ключів, що використовуються в ІТС ЦЗО, здійснюються в частині, що не суперечить вимогам цього Регламенту, відповідно до положень Інструкції із забезпечення безпеки експлуатації засобу криптографічного захисту інформації та Інструкції щодо порядку генерації ключових даних і поводження (обліку, зберігання, знищення) з ключовими документами, передбачених Положенням про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженим наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20 липня 2007 року № 141, зареєстрованим в Міністерстві юстиції України 30 липня 2007 року за № 862/14129 (із змінами), до відповідних засобів криптографічного захисту інформації (далі – КЗІ) зі складу ІТС ЦЗО, які погоджуються з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України.

2. Генерація особистих та відкритих ключів

2.1. В ІТС ЦЗО генеруються особистий та відповідний йому відкритий ключі ЦЗО для накладення та перевірки ЕЦП на сертифікатах ключів ЦЗО, Центрів та СВС, особистий та відповідний йому відкритий ключі ЦЗО для накладення та перевірки ЕЦП на даних про статус сертифікатів ключів Центрів, що визначається в режимі реального часу, особистий та відповідний йому відкритий ключі шлюзу захисту мережевих з'єднань, особистий та відповідний йому відкритий ключі адміністраторів (далі разом – особисті та відповідні їм відкриті ключі ЦЗО).

2.2. Генерація особистих та відповідних їм відкритих ключів ЦЗО здійснюється у спеціальному приміщенні ІТС ЦЗО за участю адміністратора сертифікації під контролем адміністратора безпеки.

Після генерації особистих та відкритих ключів ЦЗО здійснюється формування відповідних сертифікатів ключів.

Особисті ключі ЦЗО для накладення ЕЦП на сертифікати ключів Центрів та СВС та особисті ключі ЦЗО для накладення ЕЦП на дані про статус сертифікатів ключів Центрів, що визначається в режимі реального часу, зберігаються відповідно в апаратних та апаратно-програмних

засобах КЗІ, що входять до складу ІТС ЦЗО.

Особисті ключі шлюзу захисту мережевих з'єднань та особисті ключі адміністраторів зберігаються на зовнішніх носіях ключової інформації (далі – НКІ).

Для забезпечення можливості відновлення особистого ключа ЦЗО для накладення ЕЦП на сертифікати ключів Центрів та СВС, особистого ключа ЦЗО для накладення ЕЦП на дані про статус сертифікатів ключів Центрів, що визначається в режимі реального часу у випадку виходу з ладу апаратних та апаратно-програмних засобів КЗІ, виконується резервне копіювання відповідного особистого ключа із засобу КЗІ на НКІ.

Для забезпечення можливості відновлення особистих ключів шлюзу захисту мережевих з'єднань та особистих ключів адміністраторів у випадку виходу з ладу НКІ виконується резервне копіювання особистого ключа із засобу КЗІ на окремі резервні НКІ.

Факти генерації та створення резервних копій особистого ключа ЦЗО для накладення ЕЦП на сертифікати ключів Центрів та СВС, особистого ключа ЦЗО для накладення ЕЦП на дані про статус сертифікатів ключів Центрів, що визначається в режимі реального часу, особистого ключа шлюзу захисту мережевих з'єднань (далі разом – особисті ключі ЦЗО), особистих ключів адміністраторів та відповідних їм відкритих ключів реєструються адміністратором безпеки у відповідному журналі обліку.

2.3. Передавання особистих ключів ЦЗО здійснюється за журналом прийому-передачі ключів.

Забороняється:

передавання особистих ключів адміністраторів між адміністраторами.

виносити особисті ключі ЦЗО та їх резервні копії із спеціального приміщення ІТС ЦЗО.

3. Планова та позапланова заміна ключів, їх знищення

3.1. Строки дії особистих ключів ЦЗО відповідають строкам чинності сертифікатів відповідних їм відкритих ключів і становлять:

для особистих ключів ЦЗО для накладення ЕЦП на сертифікатах ключів ЦЗО, Центрів та СВС не більше 10 років;

для особистих ключів ЦЗО для накладення ЕЦП на дані про статус сертифікатів ключів Центрів, що визначається в режимі реального часу, не більше 5 років;

для особистих ключів шлюзу захисту мережевих з'єднань не більше 2 років.

Строк дії особистих ключів адміністраторів становить не більше 2 років.

3.2. Планова заміна особистого та відповідного йому відкритого ключа ЦЗО виконується не пізніше ніж за 2 робочі дні до закінчення строку дії відповідного сертифіката ключа.

Під час планової заміни особистого та відповідного йому відкритого ключа ЦЗО адміністратором сертифікації під контролем адміністратора безпеки відповідно до вимог пункту 2.2 глави 2 цього розділу здійснюється генерація нових особистого та відповідного йому відкритого ключа ЦЗО, формування відповідного сертифіката ключа та створення резервних копій особистого ключа.

Після введення в дію нових особистого та відповідного йому відкритого ключа ЦЗО особистий ключ, термін дії сертифіката відкритого ключа якого завершився, та всі його резервні копії знищуються методом, що не допускає можливості їх відновлення, за участю двох адміністраторів, у тому числі адміністратора безпеки.

3.3. Позапланова заміна особистого та відповідного йому відкритого ключа ЦЗО виконується у випадках компрометації або підозри на компрометацію особистого ключа ЦЗО та/або особистого ключа адміністратора.

Під час позапланової заміни особистого та відповідного йому відкритого ключа ЦЗО адміністратором сертифікації під контролем адміністратора безпеки відповідно до вимог пункту 2.2 глави 2 цього розділу здійснюється генерація нових особистого та відповідного йому відкритого ключа ЦЗО, формування відповідного сертифіката ключа та створення резервних копій особистого ключа.

У разі підтвердження факту компрометації особистих ключів ЦЗО для накладення ЕЦП на сертифікати ключів Центрів та СВС усі попередньо сформовані сертифікати ключів Центрів скасовуються та формується СВС, який підписується новим особистим ключем ЦЗО для накладення ЕЦП на сертифікати ключів Центрів та СВС.

Усі особисті ключі ЦЗО та особисті ключі адміністраторів, факт компрометації яких було підтверджено, знищуються методом, що не допускає можливості їх відновлення, за участю двох адміністраторів, у тому числі адміністратора безпеки.

3.4. ЦЗО невідкладно інформує Центри та контролюючий орган про здійснення планової чи позапланової заміни особистих та відкритих ключів ЦЗО.

4. Особливості планової заміни особистого ключа ЦЗО для накладення ЕЦП на сертифікати ключів ЦЗО, Центрів та СВС

4.1. Не пізніше завершення половини строку дії поточного особистого та відповідного йому відкритого ключа ЦЗО для накладення та перевірки ЕЦП на сертифікатах ключів ЦЗО, Центрів та СВС здійснюється генерація нового особистого та відповідного йому відкритого ключа ЦЗО для накладення та перевірки ЕЦП на сертифікатах ключів ЦЗО, Центрів та СВС та формування відповідного сертифіката ключа. При цьому поточний особистий ключ ЦЗО для накладення ЕЦП на сертифікати ключів ЦЗО, Центрів та СВС стає попереднім, а новий – поточним.

Поточний особистий ключ ЦЗО для накладення ЕЦП на сертифікати ключів ЦЗО, Центрів та СВС повинен зберігатися і застосовуватися в апаратному засобі КЗІ, що входить до складу ІТС ЦЗО, та використовуватися для накладення ЕЦП на сертифікати ключів Центрів і СВС.

Попередній особистий ключ ЦЗО для накладення ЕЦП на сертифікати ключів ЦЗО, Центрів та СВС повинен зберігатися і застосовуватися в апаратно-програмному засобі КЗІ, що входить до складу ІТС ЦЗО, та використовуватися для накладення ЕЦП тільки для обслуговування сертифікатів ключів Центрів, які були сформовані за допомогою цього ключа.

4.2. Перенесення попереднього особистого ключа ЦЗО для накладення ЕЦП на сертифікати ключів ЦЗО, Центрів та СВС з апаратного до апаратно-програмного засобу КЗІ здійснюється шляхом створення резервної копії особистого ключа ЦЗО для накладення ЕЦП на сертифікати ключів ЦЗО, Центрів та СВС та її відновлення.

Факти створення та відновлення резервної копії попереднього особистого ключа ЦЗО для накладення ЕЦП на сертифікати ключів ЦЗО, Центрів та СВС та його перенесення з апаратного засобу КЗІ до апаратно-програмного засобу КЗІ реєструються адміністратором безпеки у відповідному журналі обліку.

Директор Департаменту нотаріату, банкрутства та функціонування центрального засвідчувального органу **К.І. Чижмарь**

З оригіналом згідно

20.02.2013

Додаток 1
до Регламенту роботи центрального
засвідчувального органу

Обов'язкові реквізити Центру
в запиті на формування сертифіката ключа

Таблиця 1

Назва реквізиту англійською мовою	Назва реквізиту українською мовою	Значення реквізиту
countryName	назва країни	країна, в якій зареєстрована організація – юридична особа або фізична особа, яка є суб'єктом підприємницької діяльності id-at-countryName AttributeType ::= {id-at 6} X520countryName ::= PrintableString (SIZE(2)) код згідно з міжнародним стандартом ISO 3166 (для України – UA)
organizationName	найменування організації	повне (або офіційне скорочене) найменування організації – юридичної особи або прізвище та ініціали фізичної особи, яка є суб'єктом підприємницької діяльності, за установчими документами або відомостями про державну реєстрацію id-at-organizationName AttributeType ::= {id-at 10} X520organizationName::= DirectoryString (SIZE(64))
serialNumber	серійний номер	унікальний реєстраційний номер Центру id-at-serialNumber AttributeType ::= {id-at 5} serialNumber::= PrintableString (SIZE(64)) Значення цього реквізиту задається згідно з пунктом 1.4 глави 1 розділу V цього Регламенту

Назва реквізиту англійською мовою	Назва реквізиту українською мовою	Значення реквізиту
stateOrProvinceName	назва області[1]	область, у якій зареєстрована організація – юридична особа або фізична особа, яка є суб'єктом підприємницької діяльності id-at-stateOrProvinceName AttributeType ::= {id-at 8} X520stateOrProvinceName ::= DirectoryString (SIZE(64))
localityName	назва міста	місто, в якому зареєстрована організація – юридична особа або фізична особа, яка є суб'єктом підприємницької діяльності id-at-localityName AttributeType ::= {id-at 7} X520localityName ::= DirectoryString (SIZE(64))
commonName	найменування Центру	найменування Центру id-at-commonName AttributeType ::= {id-at 3} X520commonName ::= DirectoryString (SIZE(64))
organizationalUnitName	назва підрозділу організації	назва підрозділу організації, що є Центром та забезпечує надання послуг ЕЦП id-at-organizationalUnitName AttributeType ::= {id-at 11} X520organizationalUnitName ::= DirectoryString (SIZE(64))

[1] Якщо місцем реєстрації юридичної особи або фізичної особи – суб'єкта підприємницької діяльності є місто Київ або Севастополь, реквізит "stateOrProvinceName" повинен бути відсутнім.

Обробка розширень, поданих у запиті під час формування сертифіката ключа Центру

Таблиця 2

Назва розширення англійською мовою	Назва розширення українською мовою (у термінології Наказу)	Обов'язковість розширення у сертифікаті ключа Центру[1]	Обов'язковість розширення у запиті[2]	Встановлення розширення у сертифікаті ключа Центру у разі його наявності у запиті[3]	Додавання розширення у сертифікаті ключа Центру у разі його відсутності у запиті[4]	Примітки
Стандартні розширення						
authorityKeyIdentifier	Ідентифікатор відкритого ключа Центру	+	+/-	-	+	Встановлюється значення ідентифікатора відкритого ключа ЦЗО
subjectKeyIdentifier	Ідентифікатор відкритого ключа підписувача	+	+/-	+	+	У разі відсутності розширення у запиті встановлюється значення ідентифікатора відкритого ключа, який обчислюється ЦЗО згідно з вимогами, встановленими Наказом
keyUsage	Призначення відкритого ключа, що міститься в сертифікаті	+	+/-	+/-	+	У разі наявності розширення у запиті аналізуються усі його значення. У сертифікаті відкритого ключа Центру встановлюються тільки ті, що визначаються сферою використання відкритого ключа Центру і зазначені у заяві на формування посиленого сертифіката відкритого ключа. У разі відсутності розширення у запиті у сертифікаті відкритого ключа Центру встановлюється значення, що визначається сферою використання відкритого ключа Центру і зазначено у заяві на формування посиленого сертифіката відкритого ключа

Назва розширення англійською мовою	Назва розширення українською мовою (у термінології Наказу)	Обов'язковість розширення у сертифікаті ключа Центру[1]	Обов'язковість розширення у запиті[2]	Встановлення розширення у сертифікаті ключа Центру у разі його наявності у запиті[3]	Додавання розширення у сертифікаті ключа Центру у разі його відсутності у запиті[4]	Примітки
extKeyUsage	Уточнене призначення відкритого ключа, що міститься в сертифікаті	+/-	+/-	+/-	+	У разі наявності розширення у запиті аналізуються усі його значення. У сертифікаті відкритого ключа Центру встановлюються тільки ті, що визначаються сферою використання відкритого ключа Центру і зазначені у заяві на формування посиленого сертифіката відкритого ключа. У разі відсутності розширення у запиті у сертифікаті відкритого ключа Центру встановлюється значення, що визначається сферою використання відкритого ключа Центру і зазначено у заяві на формування посиленого сертифіката відкритого ключа
certificatePolicies	Політика сертифікації	+	+/-	+/-	+	У разі наявності та відповідності значення розширення у запиті, що відповідає політиці сертифікації ЦЗО, у сертифікаті відкритого ключа Центру встановлюється значення розширення, що міститься у запиті на його формування. У разі відсутності або відмінності значення розширення у запиті на формування сертифіката від значення, що відповідає політиці сертифікації ЦЗО, встановлюється значення, що відповідає політиці сертифікації ЦЗО
subjectAltName	Додаткові дані підписувача	+/-	+/-	+	-	Встановлюється значення розширення у сертифікаті відкритого ключа Центру, що міститься у запиті на його формування

Назва розширення англійською мовою	Назва розширення українською мовою (у термінології Наказу)	Обов'язковість розширення у сертифікаті ключа Центру[1]	Обов'язковість розширення у запиті[2]	Встановлення розширення у сертифікаті ключа Центру у разі його наявності у запиті[3]	Додавання розширення у сертифікаті ключа Центру у разі його відсутності у запиті[4]	Примітки
issuerAlternativeName	Додаткові дані Центру	+/-	+/-	-	-	
basicConstraints	Основні обмеження	+/-	+/-	+/-	+	У разі наявності та відповідності значення розширення у запиті на формування сертифіката значенню, що відповідає вимогам Наказу, встановлюється значення розширення, що міститься у запиті на його формування. У разі відсутності або відмінності значення розширення у запиті на формування сертифіката від значення, що визначено Наказом, встановлюється значення, що відповідає ЗЦ, ЦСК або АЦСК згідно з Наказом
subjectDirectoryAttributes	Персональні дані підписувача	+/-	+/-	+	-	Встановлюється значення розширення у сертифікаті відкритого ключа Центру, що міститься у запиті на його формування
crlDistributionPoints	Точки доступу до СВС	+/-	+/-	-	+	Встановлюються значення, що відповідають адресам точок доступу до повних СВС ЦЗО
freshestCRL	Точки доступу до часткового СВС	+/-	+/-	-	+	Встановлюються значення, що відповідають адресам точок доступу до часткових СВС ЦЗО

Назва розширення англійською мовою	Назва розширення українською мовою (у термінології Наказу)	Обов'язковість розширення у сертифікаті ключа Центру[1]	Обов'язковість розширення у запиті[2]	Встановлення розширення у сертифікаті ключа Центру у разі його наявності у запиті[3]	Додавання розширення у сертифікаті ключа Центру у разі його відсутності у запиті[4]	Примітки
Нестандартні розширення						
qcStatements	Ознаки посиленого сертифіката	+/-	+/-	+/-	+	У разі наявності та відповідності значення розширення у запиті на формування сертифіката значенню, що відповідає вимогам Наказу, встановлюється значення розширення, що міститься у запиті на його формування. У разі відсутності або відмінності значення розширення у запиті на формування сертифіката від значення, що відповідає політиці сертифікації ЦЗО, встановлюється значення, що відповідає політиці сертифікації ЦЗО

[1] Обов'язковість розширення у сертифікаті ключа Центру:

+ - розширення обов'язкове;

+/- - розширення може бути присутнім або відсутнім.

[2] Обов'язковість розширення у запиті:

+ - розширення обов'язкове;

+/- - розширення може бути присутнім або відсутнім.

[3] Встановлення розширення у сертифікаті ключа Центру у разі його наявності у запиті:

- - розширення не встановлюється у сертифікаті ключа Центру;

+ - розширення встановлюється у сертифікаті ключа Центру;

+/- - розширення може встановлюватися або не встановлюватися у сертифікаті ключа Центру.

[4] Додавання розширення у сертифікаті ключа Центру у разі його відсутності у запиті:

- - розширення не встановлюється у сертифікаті ключа Центру;

+ - розширення встановлюється у сертифікаті ключа Центру.

З оригіналом згідно

Міністерство юстиції України
Управління документального забезпечення

Гол. спеціаліст
Упр. документального забезпечення
20.02.2013 Т.Ю. Хорошевська

КОПІЯ

Додаток 2
до Регламенту роботи
центрального засвідчувального
органу

Вихідний номер_____

Дата _____

ЗАЯВА

на проведення реєстрації

Заявник _____,
(повне найменування юридичної особи,
прізвище, ім'я та по батькові (для фізичної особи, яка є суб'єктом підприємницької діяльності))

_____,
(посада, прізвище, ім'я та по батькові керівника юридичної особи,
серія і номер паспорта, ким і коли виданий (для фізичної особи, яка є суб'єктом підприємницької діяльності))

організаційно-правова форма _____,

код згідно з ЄДРПОУ _____,
(для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки платника податків з Державного реєстру фізичних осіб – платників податків)

_____,
(місце реєстрації юридичної особи, фізичної особи – суб'єкта підприємницької діяльності)

банківські реквізити:_____
(номер поточного (для банків – кореспондентського) рахунку)

_____, _____,
(МФО) (найменування банку)

номери телефонів _____,

електронна адреса інформаційного ресурсу _____,

адреса електронної пошти _____.

Відомості про контактну особу:

_____,
(прізвище, ім'я та по батькові)

_____,
(посада)

номери телефонів _____,

адреса електронної пошти _____.

1. Просимо внести реєстраційні дані, зазначені у заяві

центру сертифікації ключів /
засвідчувального центру
(необхідне підкреслити)

_____,
(назва центру сертифікації ключів, засвідчувального центру)

до Реєстру суб'єктів, які надають послуги, пов'язані з електронним цифровим підписом.

2. До заяви додаються: _____
(перелік документів, що додаються до заяви)

_____

_____

_____

_____

_____

_____

_____ _____
(підпис) (посада, прізвище та ініціали керівника юридичної особи (прізвище та ініціали – для фізичної особи, яка є суб'єктом підприємницької діяльності) або його уповноваженої особи)

"___" _____ 20___ року

М.П. З оригіналом згідно

Гол. спеціаліст відділу документального забезпечення 20.02.2018

МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ УПРАВЛІННЯ ДОКУМЕНТАЛЬНОГО ЗАБЕЗПЕЧЕННЯ

Л. Кудасовська

КОПІЯ

Додаток 3
до Регламенту роботи
центрального засвідчувального
органу

Вихідний номер_____

Дата _____

ЗАЯВА

на проведення акредитації

Заявник _____,
(повне найменування юридичної особи,
прізвище, ім'я та по батькові (для фізичної особи, яка є суб'єктом підприємницької діяльності))

_____,
(посада, прізвище, ім'я та по батькові керівника юридичної особи,
серія і номер паспорта, ким і коли виданий (для фізичної особи, яка є суб'єктом підприємницької діяльності))

організаційно-правова форма _____,

код згідно з ЄДРПОУ _____,
(для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки
платника податків з Державного реєстру фізичних осіб – платників податків)

_____,
(місце реєстрації юридичної особи, фізичної особи – суб'єкта підприємницької діяльності)

банківські реквізити:_____
(номер поточного (для банків – кореспондентського) рахунку)

_____, _____,
(МФО) (найменування банку)

номери телефонів _____,

електронна адреса інформаційного ресурсу _____,

адреса електронної пошти _____.

Відомості про контактну особу:

_____,
(прізвище, ім'я та по батькові)

_____,
(посада)

номери телефонів _____,
адреса електронної пошти _____.

1. Просимо провести акредитацію у Центральному засвідчувальному органі

центру сертифікації ключів/
акредитованого центру сертифікації ключів (у випадку переакредитації)/
засвідчувального центру

(необхідне підкреслити)

_____,
(назва центру сертифікації ключів, акредитованого центру сертифікації ключів, засвідчувального центру)

реєстраційний номер сформованого Центральним засвідчувальним органом посиленого сертифіката відкритого ключа якого: _____

Свідоцтво про акредитацію (у випадку переакредитації) від _____20___ року № _____.

2. Заявляємо, що

_____
(назва центру сертифікації ключів, акредитованого центру сертифікації ключів, засвідчувального центру)

відповідає встановленим Порядком акредитації центру сертифікації ключів, затвердженим постановою Кабінету Міністрів України від 13 липня 2004 року № 903, Правилами посиленої сертифікації, затвердженими наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3, зареєстрованими у Міністерстві юстиції України 27 січня 2005 року за № 104/10384, та Регламентом _____
(назва Регламенту)

вимогам.

3. Зобов'язуємося виконувати всі правила та процедури акредитації і забезпечувати відповідність вимогам законодавства _____

_____.
(назва центру сертифікації ключів, акредитованого центру сертифікації ключів, засвідчувального центру)

4. До заяви додаються: _____
(перелік документів, що додаються до заяви)

_____

_____

_____

_____ _____
(підпис) (посада, прізвище та ініціали керівника юридичної особи (прізвище та ініціали – для фізичної особи, яка є суб'єктом підприємницької діяльності) або його уповноваженої особи)

„___" _____ 20___року

М.П.

Заповнює посадова особа Центрального засвідчувального органу

Дата отримання _____ **Дата реєстрації** _____

Службові відмітки _____

_____

З оригіналом згідно

Гол. спец. відділу УВД документації Управління 20.02.2023

МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ УПРАВЛІННЯ ДОКУМЕНТАЛЬНОГО ЗАБЕЗПЕЧЕННЯ

Т. Худаковська

КОПІЯ

Додаток 4
до Регламенту роботи
центрального засвідчувального
органу

Вихідний номер_____

Дата _____

ЗАЯВА

на формування посиленого сертифіката відкритого ключа

Центр сертифікації ключів

Акредитований центр сертифікації ключів

Засвідчувальний центр

(необхідне підкреслити)

_____,
(повне найменування юридичної особи,
прізвище, ім'я та по батькові (для фізичної особи, яка є суб'єктом підприємницької діяльності))

_____,
(посада, прізвище, ім'я та по батькові керівника юридичної особи,
серія і номер паспорта, ким і коли виданий (для фізичної особи, яка є суб'єктом підприємницької діяльності))

організаційно-правова форма _____,

код згідно з ЄДРПОУ _____
(для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки
платника податків з Державного реєстру фізичних осіб – платників податків)

_____,
(місце реєстрації юридичної особи, фізичної особи – суб'єкта підприємницької діяльності)

номери телефонів _____,

електронна адреса інформаційного ресурсу _____,

адреса електронної пошти _____.

1. Просимо перевірити унікальність належного нам відкритого ключа, що міститься в запиті на формування сертифіката, за відомостями реєстру чинних, блокованих та скасованих сертифікатів ключів Центрів.

2. Просимо перевірити унікальність у межах України сформованого нами розпізнавального імені UA-_____
(розпізнавальне ім'я)

3. Просимо сформувати посилений сертифікат відкритого ключа

_____
(назва центру сертифікації ключів, акредитованого центру сертифікації ключів, засвідчувального центру)

відповідно до запиту на сертифікат: _____
(назва файла)

з такими даними:

CN (commonName) = Загальна назва = _____
OU (organizationUnit-Name) = Підрозділ = _____
O (organizationName) = Організація = _____
L (localityName) = Місто = _____
S (stateOrProvinceName) = Область = _____
C (countryName) = Країна = UA

Значення серійного (заводського) номера носія інформації, на якому надаємо запит на формування сертифіката: _____.

_____ _____
(підпис) (посада, прізвище та ініціали керівника юридичної особи (прізвище та ініціали – для фізичної особи, яка є суб'єктом підприємницької діяльності) або його уповноваженої особи)

„___" _____ 20___року

М.П. З оригіналом згідно

Гол. спеціаліст упр. документального забезпечення 20.01.2023

Міністерство юстиції України Управління документального забезпечення

А. Худаковська

КОПІЯ

Додаток 5
до Регламенту роботи
центрального засвідчувального
органу

Вихідний номер_____

Дата _____

ЗАЯВА

на скасування посиленого сертифіката відкритого ключа

Центр сертифікації ключів

Акредитований центр сертифікації ключів

Засвідчувальний центр

(необхідне підкреслити)

_____,
(повне найменування юридичної особи,
прізвище, ім'я та по батькові (для фізичної особи, яка є суб'єктом підприємницької діяльності))

_____,
(посада, прізвище, ім'я та по батькові керівника юридичної особи,
серія і номер паспорта, ким і коли виданий (для фізичної особи, яка є суб'єктом підприємницької діяльності))

код згідно з ЄДРПОУ _____,
(для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки
платника податків з Державного реєстру фізичних осіб – платників податків)

номери телефонів _____,

електронна адреса інформаційного ресурсу _____,

адреса електронної пошти _____.

У зв'язку із _____
(причина скасування посиленого сертифіката відкритого ключа)

_____

просимо скасувати посилений сертифікат відкритого ключа

_____,
(назва центру сертифікації ключів, акредитованого центру сертифікації ключів, засвідчувального центру)

серійний номер якого: _____

_____ _____
(підпис) (посада, прізвище та ініціали керівника юридичної особи (прізвище та ініціали – для фізичної особи, яка є суб'єктом підприємницької діяльності) або його уповноваженої особи чи посадових осіб державної виконавчої служби або контролюючого органу у випадках, передбачених статтею 13 Закону України «Про електронний цифровий підпис»)

„___" _____ 20___року

М.П.

З оригіналом згідно

Гол. спеціаліст
упр. документ.
забезпечення
20.03.2013

МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ
УПРАВЛІННЯ ДОКУМЕНТАЛЬНОГО ЗАБЕЗПЕЧЕННЯ

Н. Ходаковська

КОПІЯ

Додаток 6
до Регламенту роботи
центрального засвідчувального
органу

Вихідний номер_____

Дата _____

ЗАЯВА

на блокування посиленого сертифіката відкритого ключа

Центр сертифікації ключів

Акредитований центр сертифікації ключів

Засвідчувальний центр
(необхідне підкреслити)

_____,
(повне найменування юридичної особи,
прізвище, ім'я та по батькові (для фізичної особи, яка є суб'єктом підприємницької діяльності))

_____,
(посада, прізвище, ім'я та по батькові керівника юридичної особи,
серія і номер паспорта, ким і коли виданий (для фізичної особи, яка є суб'єктом підприємницької діяльності))

код згідно з ЄДРПОУ _____,
(для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки
платника податків з Державного реєстру фізичних осіб – платників податків)

номери телефонів _____,

електронна адреса інформаційного ресурсу _____,

адреса електронної пошти _____.

У зв'язку із _____
(причина блокування посиленого сертифіката відкритого ключа)

_____

просимо блокувати посилений сертифікат відкритого ключа

_____,
(назва центру сертифікації ключів, акредитованого центру сертифікації ключів, засвідчувального центру)

серійний номер якого: _____

_____ _____
(підпис) (посада, прізвище та ініціали керівника юридичної особи (прізвище та ініціали – для фізичної особи, яка є суб'єктом підприємницької діяльності) або його уповноваженої особи чи посадових осіб державної виконавчої служби або контролюючого органу у випадках, передбачених статтею 13 Закону України «Про електронний цифровий підпис»)

„___" _____ 20___року

М.П.

З оригіналом згідно

Гол. спец. 1 кат. упр. документ. забезпечення 20.02.2023

Міністерство юстиції України Управління документального забезпечення

Т. Ходаковська

КОПІЯ

Додаток 7
до Регламенту роботи
центрального засвідчувального
органу

Вихідний номер_____

Дата _____

ЗАЯВА

на поновлення посиленого сертифіката відкритого ключа

Центр сертифікації ключів

Акредитований центр сертифікації ключів

Засвідчувальний центр

(необхідне підкреслити)

_____,
(повне найменування юридичної особи,
прізвище, ім'я та по батькові (для фізичної особи, яка є суб'єктом підприємницької діяльності))

_____,
(посада, прізвище, ім'я та по батькові керівника юридичної особи,
серія і номер паспорта, ким і коли виданий (для фізичної особи, яка є суб'єктом підприємницької діяльності))

код згідно з ЄДРПОУ _____,
(для фізичної особи, яка є суб'єктом підприємницької діяльності, – реєстраційний номер облікової картки
платника податків з Державного реєстру фізичних осіб – платників податків)

номери телефонів _____,

електронна адреса інформаційного ресурсу _____,

адреса електронної пошти _____.

У зв'язку із _____
(причина поновлення блокованого посиленого сертифіката відкритого ключа)

_____

просимо поновити блокований посилений сертифікат відкритого ключа

_____,
(назва центру сертифікації ключів, акредитованого центру сертифікації ключів, засвідчувального центру)

серійний номер якого: _____

_____ _____
(підпис) (посада, прізвище та ініціали керівника юридичної особи (прізвище та ініціали – для фізичної особи, яка є суб'єктом підприємницької діяльності) або його уповноваженої особи)

„___" _____ 20___року

М.П.

З оригіналом згідно

Гол. спеціаліст
Упр. документального
забезпечення
20.02.2013

МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ
УПРАВЛІННЯ ДОКУМЕНТАЛЬНОГО ЗАБЕЗПЕЧЕННЯ

А. Ходаковська