ПОГОДЖЕНО
Заступник Голови Державної
служби спеціального зв'язку та захисту
інформації України

_____ Петро ОПАЛЕНИК
«02» 03 2020 р.

ЗАТВЕРДЖУЮ
Генеральний директор
Державного підприємства
«Українські спеціальні системи»

_____ Микола СОКИРКО
«___» _____ 2020 р.

Прим. № ___

РЕГЛАМЕНТ РОБОТИ
КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ ДЕРЖАВНОГО ПІДПРИЄМСТВА «УКРАЇНСЬКІ СПЕЦІАЛЬНІ СИСТЕМИ»

ПОГОДЖЕНО
Начальник центру сертифікації ключів
ДП «Українські спеціальні системи»

_____ Віктор ІЛЬЇЧОВ
«10» 03 2020 року.

Київ-2020

ЗМІСТ

С.

ВСТУП

Цей документ є нормативним документом, що визначає організаційно-методологічні та технологічні умови діяльності кваліфікованого надавача електронних довірчих послуг (далі – КНЕДП, Надавач) Державного підприємства «Українські спеціальні системи», під час надання кваліфікованих електронних довірчих послуг (далі – довірчі послуги) та є Регламентом роботи КНЕДП Державного підприємства «Українські спеціальні системи» (далі – Регламент).

Регламент визначає порядок та процедури обслуговування кваліфікованих сертифікатів відкритих ключів (далі – сертифікат, сертифікат ключа) користувачів кваліфікованих електронних довірчих послуг (далі – КЕДП), умови надання послуг та правил користування КЕДП, а також основні організаційно-технічні заходи, що направлені на забезпечення функціонування КНЕДП.

Регламент розроблено відповідно до чинного законодавства України у сфері електронних довірчих послуг.

1. СФЕРА ЗАСТОСУВАННЯ

1.1. Регламент визначає організаційно-методологічні та технологічні умови діяльності Державного підприємства «Українські спеціальні системи» під час надання електронних довірчих послуг.

1.2. Регламент призначений для застосування суб'єктами, визначеними пунктом 1.6 цього документу.

1.3. Вимоги Регламенту є обов'язковими для виконання всіма суб'єктами, які в ньому визначені, а також є засобом офіційного повідомлення і інформування усіх суб'єктів у взаєминах, що виникають в процесі надання і використання послуг кваліфікованого електронного підпису (далі – КЕП), що надаються КНЕДП.

1.4. Будь-яка заінтересована особа може ознайомитися з положеннями Регламенту (або витягу з нього) на електронному інформаційному ресурсі, в офісах КНЕДП та його відокремлених пунктах реєстрації.

1.5. Застосування положень Регламенту засноване на його добровільному визнанні взаємодіючими сторонами. Добровільне визнання Регламенту іншою стороною є підставою для укладення договору (угоди) про взаємодію і надання відповідних послуг.

1.6. Норми Регламенту поширюються на:

- Надавача;
- відокремлені пункти реєстрації Надавача (далі – ВПР);
- користувачів КЕДП.

2 НОРМАТИВНІ ПОСИЛАННЯ

У Регламенті є посилання на такі нормативно-правові документи:

2.1. Закон України від 05.10.2017 року № 2155-VIII «Про електронні довірчі послуги».

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

2.3. Постанова Кабінету Міністрів України від 07.11.2018 №992 «Про затвердження Вимог у сфері електронних довірчих послуг» та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг»;

2.4. Постанова Кабінету Міністрів України від 19.09.2018 №749 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності»;

2.5. Закон України «Про забезпечення прав і свобод внутрішньо переміщених осіб»;

2.6. Постанови Кабінету Міністрів України від 05.11.2014 № 637 «Про здійснення соціальних виплат внутрішньо переміщеним особам»;

2.7. Постанови Кабінету Міністрів України від 14.03.2016 № 167 «Про внесення змін до деяких постанов Кабінету Міністрів України»;

2.8. Положення про порядок емісії електронних платіжних засобів і здійснення операцій з їх використанням, затвердженого постановою правління Національного банку України від 05.11.2014 року № 705;

2.9. Порядок емісії платіжних карток, які одночасно є пенсійним посвідченням, затверджений Постановою правління Пенсійного фонду України від 08.04.2016 № 7-1 зареєстрованого в Міністерстві юстиції України 26.04.2016 року за № 633/28763 (із змінами);

2.10. Порядок оформлення, виготовлення та видачі документів, що підтверджують призначення особі пенсії, затвердженого постановою правління Пенсійного фонду України від 03.11.2017 № 26-1, зареєстрованого в Міністерстві юстиції України 04.12.2017 року за № 1464/31332 (із змінами);

Інші нормативно-правові акти сфери надання електронних довірчих послуг та питань криптографічного та технічного захисту інформації.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У Регламенті використано терміни, в такому значенні:

автентифікація - електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-телекомунікаційної системи та/або походження та цілісність електронних даних;

відокремлений пункт реєстрації - представництво (філія, підрозділ, територіальний орган) надавача електронних довірчих послуг або юридична чи фізична особа, яка на підставі наказу надавача електронних довірчих послуг (його керівника) або договору, укладеного з ним, здійснює реєстрацію підписувачів з дотриманням вимог цього Закону та законодавства у сфері захисту інформації;

кваліфікований електронний підпис - удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа;

кваліфікований надавач електронних довірчих послуг - юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа - підприємець, яка надає одну або більше електронних довірчих послуг, діяльність якої відповідає вимогам цього Закону та відомості про яку внесені до Довірчого списку;

кваліфікований сертифікат відкритого ключа - сертифікат відкритого ключа, який видається кваліфікованим надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом і відповідає вимогам цього Закону;

компрометація особистого ключа - будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа;

користувачі електронних довірчих послуг - підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних, інші фізичні та юридичні особи, які отримують електронні довірчі послуги у надавачів таких послуг відповідно до вимог цього Закону, в тому числі власники електронного пенсійного посвідчення.

особистий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;

програмно-технічний комплекс, що використовується під час надання електронних довірчих послуг (далі - програмно-технічний комплекс), - апаратні, апаратно-програмні та програмні засоби, що забезпечують виконання функцій, пов’язаних з наданням електронних довірчих послуг;

Інші терміни вживаються в значеннях встановлених в нормативно-правових актах визначених у Розділі 2 Регламенту.

4. ПОЗНАЧКИ ТА СКОРОЧЕННЯ

ВПР – відокремлений пункт реєстрації;
КНЕДП – кваліфікований надавач електронних довірчих послуг Державного підприємства «Українські спеціальні системи»;
ЦЗО – центральний засвідчувальний орган;
КЕП – кваліфікований електронний підпис чи печатка;
КЕДП – кваліфікована електронна довірча послуга;
РНОКПП – реєстраційний номеру облікової картки платника податків;
ЄДДР – єдиний державний демографічний реєстр;
ПТК – програмно-технічний комплекс;
ІТС – інформаційно-телекомунікаційна система;
СЗІ – служба захисту інформації;
СВС – список відкликаних сертифікатів;
ЦОД – центр обробки даних;
БД – база даних;
НКІ – носій ключової інформації – програмно-апаратний засіб КЕП;
ПЗ – програмне забезпечення;
HTTP – «Hyper Text Transfer Protocol» (протокол прикладного рівня, що використовується для передавання гіпертексту;
TSP – «Time Stamp Protocol» (протокол фіксування часу);
CMP – «Certificate Management Protocol» (протокол управління
OCSP сертифікатами);
– «Online Certificate Status Protocol» (протокол визначення
URL статусу сертифіката ключа);
– «Unique resource locator» (унікальна адреса інформаційного ресурсу в телекомунікаційній мережі).

5. ЗАГАЛЬНІ ВІДОМОСТІ

5.1 Ідентифікаційні дані КНЕДП

Країна	Україна
Назва області	Київська
Назва міста	Київ
Повні найменування організації	ДЕРЖАВНЕ ПІДПРИЄМСТВО «УКРАЇНСЬКІ СПЕЦІАЛЬНІ СИСТЕМИ», THE STATE ENTERPRISE «UKRAINIAN SPECIAL SYSTEMS».
Скорочені найменування організації	ДП «УСС», SE «USS».
Юридична адреса	04119, м. Київ, вул. Юрія Іллєнка, 83Б
Поштова адреса	04119, м. Київ, вул. Юрія Іллєнка, 83Б
Адреса місцезнаходження	04119, м. Київ, вул. Юрія Іллєнка, 83Б
Код ЄДРПОУ	32348248
Повне найменування	Кваліфікований надавач електронних довірчих послуг Державного підприємства «Українські спеціальні системи»
Номери телефонів	+38 (044) 481-49-63, +38 (044) 481-49-50, +38 (063) 343-16-61 в неробочий час (з питань блокування та поновлення сертифікатів +38 (044) 481-49-61).
Електронна пошта	csk@uss.gov.ua
Електронна адреса	https://csk.uss.gov.ua

Надавач представлений окремим підрозділом або позаштатною структурою
ДП «УСС», що здійснює надання кваліфікованих електронних довірчих послуг з дотриманням вимог законодавства.

Представництвами надавача є відокремлені пункти реєстрації, що представлені окремими підрозділами або позаштатними одиницями ДП «УСС», які підпорядковані Надавачу, або юридичні чи фізичні особи, які на підставі договору з ДП «УСС», здійснюють реєстрацію користувачів електронних довірчих послуг з дотриманням вимог законодавства сферах електронних довірчих послуг та захисту інформації.

Надавач бере участь в реалізації повноважень визначених нормативно-правовими актами, викладеними в пунктах 2.5.-2.10. Розділу 2 Регламенту.

Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені ДП «УСС» або від імені представництва.

5.2 Порядок публікації

Положення Регламенту розповсюджується:

- в електронній формі:

з веб-сайту КНЕДП за адресою https://csk.uss.gov.ua;

засобами електронної пошти від уповноваженої особи КНЕДП;

- у паперовій формі:

через поштову адресу: 04119, м. Київ, вул. Юрія Іллєнка, 83Б.

5.3 Порядок внесення змін та доповнень

Внесення змін та доповнень до Регламенту здійснюється КНЕДП у відповідності до чинного законодавства України.

Про внесення змін та доповнень до Регламенту КНЕДП повідомляє користувачів та інших зацікавлених осіб офіційним повідомленням. Офіційне повідомлення здійснюється у спосіб, визначений у п. 5.2 «Порядок публікації».

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

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

Договори та інші правочини, умови яких суперечать змінам чи доповненням до цього документу, повинні бути переукладені протягом 10 (десяти) робочих днів з дня набрання чинності таких змін.

6. ПЕРЕЛІК КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, НАДАННЯ ЯКИХ ЗАБЕЗПЕЧУЄ КНЕДП

1) Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки;

2) Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;

3) Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу.

7. ПЕРЕЛІК ПОСАД ТА ФУНКЦІЇ НАЙМАНИХ ПРАЦІВНИКІВ

7.1. Працівниками Надавача, посадові обов’язки яких безпосередньо пов’язані з наданням кваліфікованих електронних довірчих послуг є:

- керівник (начальник) КНЕДП;
- адміністратор реєстрації;
- адміністратор сертифікації;
- адміністратор безпеки та аудиту;
- системний адміністратор.

7.2. Керівник (начальник) КНЕДП відповідає за керування підрозділом, вчасне та якісне виконання покладених на нього функціональних завдань. В межах виконання своїх обов'язків відповідає за організацію та контроль процесів, направлених на забезпечення функціонування, розвитку надавача та захист інформації в інформаційно-телекомунікаційній системі (далі – ІТС) Надавача, а саме:

- контроль за виконанням регламентних процедур з експлуатації та технічного обслуговування ІТС Надавача;
- контроль за впровадженням та забезпеченням функціонування комплексної системи захисту інформації ІТС Надавача;
- контроль за забезпеченням працездатності загальносистемного та спеціального програмного ІТС Надавача;
- забезпечення актуалізації баз даних, створюваних та оброблюваних в ІТС Надавача;
- розгляд та оцінка технічних рішень щодо модернізації ІТС Надавача;
- розробка та узгодження технічних завдань, проектної та експлуатаційної документації ІТС Надавача та комплексної системи захисту інформації ІТС Надавача;
- контроль за будівельно-монтажними та пусконалагоджувальними роботами;
- проведення попередніх випробувань, дослідної експлуатації та введення ІТС Надавача в експлуатацію;

7.3. Адміністратор реєстрації відповідає за перевірку документів, наданих заявниками, їх заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів.

Основними обов’язками адміністратора реєстрації є:

- ідентифікація та автентифікація заявників;
- перевірка заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів;
- встановлення належності відкритого ключа та відповідного йому особистого ключа заявнику;
- ведення обліку користувачів.

До працівників відокремлених пунктів реєстрації, на яких покладено обов’язки з реєстрації користувачів, застосовуються такі ж вимоги, як і до адміністраторів реєстрації.

7.4. Адміністратор сертифікації відповідає за формування кваліфікованих сертифікатів відкритих ключів, ведення електронного реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів, збереження та використання особистих ключів надавача, а також створення їх резервних копій.

Основними обов'язками адміністратора сертифікації є:

- участь у генерації пар ключів надавача та створенні резервних копій особистих ключів Надавача;
- зберігання особистих ключів Надавача та їх резервних копій;
- забезпечення використання особистих ключів Надавача під час формування та обслуговування кваліфікованих сертифікатів відкритих ключів надавача та користувачів;
- перевірка заяв про формування кваліфікованих сертифікатів відкритих ключів надавача на відповідність вимогам регламенту роботи Надавача;
- участь у знищенні особистих ключів Надавача;
- забезпечення ведення, архівування та відновлення баз даних кваліфікованих сертифікатів відкритих ключів користувачів;
- забезпечення публікації кваліфікованих сертифікатів відкритих ключів користувачів та списків відкликаних сертифікатів на офіційному веб-сайті Надавача;
- створення резервних копій кваліфікованих сертифікатів відкритих ключів користувачів;
- зберігання кваліфікованих сертифікатів відкритих ключів користувачів, їх резервних копій, списків відкликаних сертифікатів та інших важливих ресурсів інформаційно-телекомунікаційної системи надавача.

7.5. Адміністратор безпеки та аудиту відповідає за належне функціонування комплексної системи захисту інформації або системи управління інформаційною безпекою.

Основними обов'язками адміністратора безпеки та аудиту є:

- участь у генерації пар ключів Надавача та створенні резервних копій особистих ключів Надавача;
- контроль за формуванням, обслуговуванням і створенням резервних копій кваліфікованих сертифікатів відкритих ключів Надавача, користувачів та списків відкликаних сертифікатів;
- контроль за зберіганням особистих ключів Надавача та їх резервних копій, особистих ключів адміністраторів;
- участь у знищенні особистих ключів Надавача, контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;
- організація розмежування доступу до ресурсів інформаційно-телекомунікаційної системи Надавача;
- забезпечення спостереження за функціонуванням комплексної системи захисту інформації або системи управління інформаційною безпекою (реєстрація подій в інформаційно-телекомунікаційній системі надавача, моніторинг подій тощо);

- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування комплексної системи захисту інформації або системи управління інформаційною безпекою після збоїв, відмов, аварій інформаційно-телекомунікаційної системи надавача;

- забезпечення режиму доступу до приміщень Надавача, в яких розміщена інформаційно-телекомунікаційна система надавача;

- ведення журналів обліку адміністратора безпеки та аудиту, визначених документацією на комплексну систему захисту інформації або звітності, що передбачена системою управління інформаційною безпекою;

- проведення перевірок журналів аудиту подій, що реєструють технічні засоби інформаційно-телекомунікаційної системи надавача;

- проведення перевірок відповідності положень внутрішньої організаційно-розпорядчої документації надавача та документації на комплексну систему захисту інформації або систему управління інформаційною безпекою;

- контроль за дотриманням найманими працівниками надавача положень внутрішньої організаційно-розпорядчої документації надавача та документації щодо комплексної системи захисту інформації або системи управління інформаційною безпекою;

- контроль за веденням баз даних Надавача;

- контроль за веденням архіву Надавача.

Адміністратор безпеки та аудиту відповідає за проведення перевірок дотримання найманими працівниками Надавача положень внутрішньої організаційно-розпорядчої документації надавача та документації щодо комплексної системи захисту інформації або системи управління інформаційною безпекою. Надавач встановлює періодичність (у днях, тижнях або місяцях) проведення таких внутрішніх перевірок, але не рідше ніж один раз на рік.

Забороняється суміщення посадових обов’язків адміністратора безпеки та аудиту з іншими посадовими обов’язками, безпосередньо пов’язаними з наданням кваліфікованих електронних довірчих послуг.

7.6. Системний адміністратор відповідає за функціонування засобів та обладнання програмно-технічного комплексу (далі – технічні засоби) інформаційно-телекомунікаційної системи надавача.

Основними обов’язками системного адміністратора є:

- організація експлуатації та технічного обслуговування інформаційно-телекомунікаційної системи надавача і адміністрування її технічних засобів;

- забезпечення функціонування офіційного веб-сайту надавача;

- участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації або системи управління інформаційною безпекою;

- ведення журналів аудиту подій, що реєструють технічні засоби інформаційно-телекомунікаційної системи надавача;

- встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення інформаційно-телекомунікаційної системи надавача;

- встановлення та налагодження штатної підсистеми резервного копіювання бази даних інформаційно-телекомунікаційної системи надавача;

- забезпечення актуалізації баз даних, створюваних та оброблюваних в інформаційно-телекомунікаційній системі надавача, у зв’язку із збоями.

8. ПОЛІТИКА СЕРТИФІКАТА

8.1 Перелік сфер, в яких дозволяється використання кваліфікованих сертифікатів відкритих ключів, сформованих КНЕДП

Кваліфіковані сертифікати відкритих ключів, які формуються КНЕДП, призначені для забезпечення діяльності фізичних та юридичних осіб (фізичних осіб – підприємців), яка здійснюється з використанням КЕП.

Кваліфікований електронний підпис, який формується та перевіряється з використанням сертифікатів ключа, що формуються КНЕДП, використовується фізичними та юридичними особами (фізичними особами – підприємцями) – суб'єктами електронного документообігу – для ідентифікації користувача, підтвердження цілісності даних в електронній формі та автентифікації.

Перелік сфер, у яких дозволяється використання сертифікатів:

Кваліфіковані сертифікати відкритих ключів, сформованих Надавачем дозволено використовувати для:

- автентифікації;
- перевірки кваліфікованого електронного підпису;
- перевірки кваліфікованої електронної печатки;
- узгодження ключів шифрування.

8.2 Обмеження щодо використання кваліфікованих сертифікатів відкритих ключів, сформованих КНЕДП

Обмеження щодо використання сформованих КНЕДП сертифікатів ключів застосовуються у відповідності до положень цього Регламенту та діючого законодавства України.

КНЕДП має право встановлювати обмеження сфери використання сформованих ним сертифікатів ключів. Інформація щодо обмеження сфери використання сертифікату ключа зазначається у сформованому сертифікаті ключа у вигляді уточненого призначення відкритого ключа.

8.3 Перелік інформації, що розміщується КНЕДП на своєму офіційному веб-сайті

На електронному інформаційному ресурсі КНЕДП розміщується наступна інформація:

- відомості про КНЕДП (фізична адреса, контактні телефони тощо), а також перелік ВПР (у разі наявності) з адресами та контактними телефонами;
- дані про внесення відомостей про КНЕДП до Довірчого списку;
- кваліфіковані сертифікати відкритих ключів КНЕДП;
- дані про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг;
- форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;
- реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;

- дані про порядок перевірки чинності кваліфікованого сертифіката відкритого ключа, у тому числі умови перевірки статусу кваліфікованого сертифіката відкритого ключа;

- перелік актів законодавства у сфері електронних довірчих послуг.

- перелік кваліфікованих електронних довірчих послуг, які надає КНЕДП.

Зазначені інформаційні об’єкти доступні цілодобово.

Електронна адреса (DNS-ім’я) електронного інформаційного ресурсу: https://csk.uss.gov.ua.

Технічною основою інформаційного ресурсу КНЕДП є сервери взаємодії, що входять до складу програмно-технічного комплексу (далі – ПТК) КНЕДП.

Довідкова інформація (регламент роботи КНЕДП, довідково-методичні матеріали щодо порядку використання електронних довірчих послуг, контактна інформація тощо) розміщується на HTTPS-сервері сервера взаємодії у вигляді набору веб-сторінок або електронних документів (з розширеннями .doc або .pdf).

Сертифікат відкритого ключа КНЕДП, сертифікати відкритих ключів користувачів, а також списки відкликаних сертифікатів розміщуються у складі веб-сторінок на HTTPS-сервері взаємодії та інформаційному дереві LDAP-каталогу на LDAP-сервері сервера взаємодії. Доступ до HTTPS-сервера здійснюється за DNS-ім’ям csk.uss.gov.ua за протоколом HTTPS (номер TCP порту – 80) . Доступ до LDAP-сервера здійснюється за DNS-ім’ям csk.uss.gov.ua за протоколом LDAP (номер TCP порту – 389).

Для розповсюдження інформації про статус сертифікатів ключів користувачів використовується механізм списку відкликаних сертифікатів та механізм визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP.

КНЕДП надає всім користувачам послугу інтерактивного визначення статусу сертифіката (в режимі реального часу). Послуга надається шляхом відправлення запиту за протоколом HTTPS на OCSP-сервер КНЕДП.

Формати запитів та відповідей протоколу інтерактивного визначення статусу сертифіката (далі – OCSP) визначаються міжнародним стандартом RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP».

8.4 Час і порядок публікації кваліфікованих сертифікатів відкритих ключів та списків відкликаних сертифікатів

8.4.1. Кваліфіковані сертифікати КНЕДП та його серверів публікуються на інформаційному ресурсі Надавача, а саме:

- сервера обробки запитів (CMP-сервера);

- сервера позначок часу (TSP-сервера);

- сервера визначення статусу сертифікатів (OCSP-сервера).

Публікація кваліфікованих сертифікатів серверів Надавача виконується одразу після їх формування.

8.4.2. Інформація щодо формування сертифікатів відкритих ключів

користувачів та самі сертифікати відкритих ключів (за згоди їх власників на опублікування своїх сертифікатів) розміщуються на електронному інформаційному ресурсі КНЕДП безпосередньо після їх формування.

8.4.3. Публікація списків відкликаних сертифікатів здійснюється на електронному інформаційному ресурсі КНЕДП одразу після їх формування безпосередньо після обробки відповідного запиту на скасування, блокування чи поновлення свого сертифікату відкритого ключа.

8.4.4. КНЕДП виконує формування списків відкликаних сертифікатів двох типів:

- повний список;
- частковий список.

Повний список формується один раз на тиждень та містить інформацію про всі відкликані сертифікати, які були сформовані в КНЕДП за допомогою чинного власного особистого ключа КНЕДП.

Частковий список формується та поширюється кожні 2 години та містить інформацію про всі відкликані сертифікати, статус яких був змінений у межах часу випуску останнього повного списку відкликаних сертифікатів та часу формування поточного часткового списку відкликаних сертифікатів.

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

Час зміни статусу кваліфікованих сертифікатів відкритих ключів синхронізований із Всесвітнім координованим часом (UTC) з точністю до однієї секунди.

Посилання на списки відкликаних сертифікатів вносяться до кваліфікованих сертифікатів відкритих ключів користувачів електронних довірчих послуг.

8.5 Механізм підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа.

Відкритий ключ заявника подається на сертифікацію виключно у вигляді самопідписаного відповідним йому особистим ключем запиту формату PKCS#10. Належність заявнику особистого ключа, що відповідає відкритому ключу, наданому на сертифікацію, підтверджується шляхом перевірки накладеного кваліфікованого електронного підпису на запиті на формування сертифіката ключа або під час генерації пари ключів одразу після ідентифікації заявника, за умови його особистої присутності.

8.6 Умови встановлення заявника (інформація, що надається заявником під час ідентифікації особи, види документів, на підставі яких встановлюється заявник, вимоги щодо особистої присутності)

8.6.1. Формування та видача кваліфікованого сертифіката відкритого ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті відкритого ключа, не допускається.

8.6.2. Ідентифікація фізичної особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа,

здійснюється виключно за умови її особистої присутності за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр (далі – ЄДДР) та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

8.6.3. Допускається ідентифікація фізичної особи КНЕДП за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката.

8.6.4. Ідентифікація іноземців здійснюється відповідно до законодавства, зокрема, посвідки на проживання особи, яка мешкає в Україні, а також національного паспорта іноземця, або документа, що його замінює.

8.6.5. Під час перевірки цивільної правоздатності та дієздатності юридичної особи КНЕДП зобов’язаний ознайомитися з інформацією про юридичну особу, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань (далі – ЄДР), а також пересвідчитися, що обсяг її цивільної правоздатності та дієздатності є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа.

8.6.6. КНЕДП під час формування та видачі кваліфікованого сертифіката відкритого ключа здійснює ідентифікацію особи уповноваженого представника юридичної особи відповідно до вимог Закону, а також перевіряє обсяг його повноважень за документом або за даними з Єдиного державного реєстру юридичних осіб, фізичних осіб - підприємців та громадських формувань, що визначають повноваження представника.

Якщо від імені юридичної особи діє колегіальний орган, до КНЕДП подається документ, у якому визначено повноваження відповідного органу та розподіл обов’язків між його членами.

8.6.7. Реєстрація заявника – представника юридичної особи

Заявник під час проведення реєстрації подає до КНЕДП наступні документи:

- заповнену заяву на формування сертифікату, підписану керівником юридичної особи, засвідчену відбитком печатки (у разі наявності); у заяві обов’язково зазначається адреса, телефон або інша інформація, що дозволяє зв'язатися з заявником;

- оригінал установчих документів (витягів із них), що містять положення про права, обов’язки, повноваження та порядок створення органів управління юридичної особи (надається тільки юридичною особою) або їх нотаріально засвідчена копія (для ознайомлення) або інші відомості відповідно до Закону України від 15.05.2003 №755-IV «Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань»;

- копія документа про обрання (призначення) керівника юридичної особи, засвідчена в установленому порядку (надається тільки юридичною особою);

- копії 1-2 сторінок (3-4 та 5-6 сторінок за наявності на них відміток) та

сторінка з відміткою про реєстрацію місця проживання з паспорту фізичної особи – заявника, засвідчені в установленому порядку;

- копія документу, що підтверджує статус (посаду) заявника, засвідчена в установленому порядку.

- парольну фразу та допоміжним питанням, яке дасть змогу її згадати;

- копія реєстраційного номеру облікової картки платника податків (далі – РНОКПП), засвідчена в установленому порядку (або копія сторінки паспорту де внесено РНОКПП відповідним органом).

Якщо через релігійні переконання фізична особа відмовилась від РНОКПП, додатково подається копія сторінки паспорту з відміткою про таку відмову, засвідчена в установленому порядку;

У разі наявності паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій з унікальним номером запису в ЄДДР, посадовими особами КНЕДП за допомогою спеціального зчитувача для ID-паспортів здійснюється зчитування та роздрукування даних (які завіряються заявником особисто) або заявником надається копія паспорту з обох боків та копія витягу з ЄДДР щодо реєстрації місця проживання, засвідчені ним в установленому порядку. У разі, якщо в паспорт внесено РНОКПП, надання окремо оригіналу (та копії) РНОКПП в паперовому вигляді не є обов'язковим.

Для фізичних осіб - нерезидентів – копія посвідки на тимчасове чи постійне місце проживання, засвідчена в установленому порядку та копія довідки про включення до Державного реєстру фізичних осіб, засвідчена в установленому порядку;

При подачі документів особа, яка подає документи до КНЕДП, повинна мати при собі оригінал паспорту та РНОКПП.

8.6.8. Реєстрація заявника – представника юридичної особи (для представників державних установ)

Для державних установ та фізичних осіб – представників державних установ, які звертаються до КНЕДП за отриманням КЕДП, надання послуг здійснюються із урахуванням вимог Постанови КМ України від 19.09.2018 №749 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності» (далі - Порядок), відповідно до якого організацію використання кваліфікованих електронних довірчих послуг у державній установі забезпечує відповідальний підрозділ, що виконує відповідні функції, або працівник, визначений рішенням такої установи (її керівника) (далі – Відповідальна особа).

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 юридичних осіб, фізичних осіб-підприємців та громадських

формувань, який знаходиться на сайті Міністерства юстиції України.

Під час проведення реєстрації, до КНЕДП подаються наступні документи (особисто або через відповідальну особу):

- заповнену заяву про формування сертифікату, підписану керівником юридичної особи (іншою особою яка має право підпису), засвідчену відбитком печатки; у заяві обов'язково зазначається адреса, телефон або інша інформація, що дозволяє зв'язатися з заявником;

- відомості відповідно до Закону України від 15.05.2003 №755-IV «Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань»;

- копія рішення (наказу) керівника установи про визначення Відповідальної особи в установі, засвідчена в установленому порядку;

- копія документа про обрання (призначення) керівника юридичної особи, засвідчена в установленому порядку;

- копії 1-2 сторінок (3-4 та 5-6 сторінок за наявності на них відміток) та сторінка з відміткою про реєстрацію місця проживання з паспорту Відповідальної особи та підписувача, засвідчені в установленому порядку;

У разі наявності паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій з унікальним номером запису в ЄДДР, посадовими особами КНЕДП за допомогою спеціального зчитувача для ID-паспортів здійснюється зчитування та роздрукування даних (які завіряються заявником особисто) або заявником надається копія паспорту з обох боків та копія витягу з ЄДДР щодо реєстрації місця проживання, засвідчені ним в установленому порядку. У разі, якщо в паспорт внесено РНОКПП, надання оригіналу (та копії) РНОКПП в паперовому вигляді не є обов'язковим;

- копія документу, що підтверджує статус (посаду) заявника, засвідчена в установленому порядку;

- парольну фразу та допоміжним питанням, яке дасть змогу її згадати;

- копія реєстраційного номеру облікової картки платника податків (далі – РНОКПП), засвідчена в установленому порядку (або копія сторінки паспорту де внесено РНОКПП відповідним органом).

Якщо через релігійні переконання фізична особа відмовилась від РНОКПП, додатково подається копія сторінки паспорту з відміткою про таку відмову, засвідчена в установленому порядку.

При подачі документів особа, яка подає документи до КНЕДП, повинна мати при собі оригінал паспорту та оригінал РНОКПП (у разі відсутності відмітки в паспорті).

8.6.9. Реєстрація заявника – фізичної особи (фізичної особи – підприємця)

- заява на формування сертифіката для фізичної особи (фізичної особи – підприємця), підписана фізичною особою (фізичною особою – підприємцем). У заяві обов'язково зазначається адреса, телефон або інша інформація, що дозволяє зв'язатися з ним;

- копії 1-2 сторінок (3-4 та 5-6 сторінок за наявності на них відміток) та сторінка з відміткою про реєстрацію місця проживання з паспорту фізичної особи (фізичної особи – підприємця) – заявника, засвідчені в установленому

порядку;

У разі наявності паспорта громадянина України у вигляді картки, що містить безконтактний електронний носій з унікальним номером запису в ЄДДР, посадовими особами КНЕДП за допомогою спеціального зчитувача для ID-паспортів здійснюється зчитування та роздрукування даних (які завіряються заявником особисто) або заявником надається копія паспорту з обох боків та копія витягу з ЄДДР щодо реєстрації місця проживання, засвідчені ним в установленому порядку. У разі, якщо в паспорт внесено РНОКПП, надання оригіналу (та копії) РНОКПП в паперовому вигляді не є обов'язковим.

Для фізичних осіб-нерезидентів – копія посвідки на тимчасове чи постійне місце проживання, засвідчена в установленому порядку копія довідки про включення до Державного реєстру фізичних осіб, засвідчена в установленому порядку.

- парольну фразу та допоміжним питанням, яке дасть змогу її згадати.

- копія реєстраційного номеру облікової картки платника податків (далі – РНОКПП), засвідчена в установленому порядку (або копія сторінки паспорту де внесено РНОКПП відповідним органом).

Якщо через релігійні переконання фізична особа відмовилась від РНОКПП, додатково подається копія сторінки паспорту з відміткою про таку відмову, засвідчена в установленому порядку.

При подачі документів особа, яка подає документи до КНЕДП, повинна мати при собі оригінал паспорту та оригінал РНОКПП (у разі відсутності відмітки в паспорті).

У випадку реєстрації працівників фізичної особи – підприємця, комплект документів надається згідно п. 8.6.7 Регламенту.

Переліки, форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги, та роз'яснення щодо їх оформлення публікуються на офіційному веб-сайті Надавача.

Для укладання договорів про надання кваліфікованих електронних довірчих послуг Надавач може отримувати від заявників інші документи, передбачені законодавством.

8.6.10. КНЕДП не приймає до розгляду документи, які мають підчистки, дописки, закреслені слова, інші незастережні виправлення або написи олівцем, а також пошкодження, внаслідок чого їхній текст не можна прочитати.

8.6.11. За результатами розгляду наданих документів адміністратор реєстрації може прийняти рішення про відмову у реєстрації у наступних випадках:

- у разі невідповідності поданого пакету документів зі встановленим КНЕДП;

- у разі подання неналежно засвідчених копій документів;

- у разі встановлення невідповідності наданих під час реєстрації даних фактичним.

8.6.12. У разі відмови у реєстрації, адміністратор реєстрації повертає надані документи заявнику з роз'ясненням причин повернення.

8.6.13. Особа, вважається встановленою, при одночасному виконанні наступних умов:

- відомості, зазначені у заяві на формування сертифіката відкритого ключа користувача, збігаються із відповідними відомостями, наведеними в представлених документах;

- представлені документи встановленого чинним законодавством вигляду та не містять ознак внесення змін до їх змісту (підчистки, затирання окремих місць, незавірені виправлення тощо).

8.6.14. Під час встановлення особи Надавач може використовувати засоби фотофіксації факту пред'явлення заявником документів, що посвідчують особу. У разі здійснення такої фотофіксації, зберігання документів здійснюється з дотриманням вимог законодавства про захист персональних даних.

8.7 Механізм автентифікації користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований КНЕДП

В КНЕДП існують наступні механізми автентифікації користувачів, які мають чинний сертифікат відкритого ключа, сформований КНЕДП:

- при особистому зверненні: паспорт або інший документ, який посвідчує особу користувача (для фізичної особи, фізичної особи-підприємця); паспорт, який посвідчує особу представника і наказ про призначення особи на посаду (для представника юридичної особи);

- при зверненні телефонною мережею загального користування: умовне таємне слово (фраза) із парольної фрази, яка відома лише користувачів (заявнику);

- при зверненні загальнодоступними телекомунікаційними мережами з використанням електронних запитів: кваліфікований електронний підпис, сформований з використанням особистого ключа користувача.

8.8 Механізм автентифікації користувачів з питання блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа

В залежності від порядку звернення щодо блокування, скасування та поновлення сертифікату ключа передбачені різні форми автентифікації користувача та перевірки законності такого звернення:

- у разі письмового звернення заявника законність звернення встановлюється за власноручним підписом уповноваженої особи користувача та печаткою організації заявника (для юридичних осіб та фізичних осіб – підприємців, у разі її наявності);

- у разі звернення користувача у електронній формі законність звернення встановлюється за кваліфікованим електронним підписом, створеним за допомогою особистого ключа користувача (до закінчення строку його чинності) та кваліфікованої електронної печатки організації заявника (для юридичних осіб та фізичних осіб – підприємців, у разі її наявності);

- у разі звернення щодо блокування сертифікату ключа в телефонному режимі законність звернення встановлюється за парольною фразою голосової автентифікації, що вказується заявником під час реєстрації;

- у разі необхідності блокування/скасування кваліфікованого сертифіката відкритого ключа, підписувач особисто подає до КНЕДП або ВПР

заяву про відповідну зміну статусу сертифікату підписану власним КЕП.

8.9 Опис фізичного середовища (опис приміщень КНЕДП, в яких розміщена інформаційно-телекомунікаційна система КНЕДП, механізми контролю доступу до них)

8.9.1Опис спеціального приміщення

8.9.1.1. Компоненти ПТК КНЕДП розміщуються у наступних приміщеннях: спеціальному приміщенні (серверне приміщення), у якому знаходиться захищена (екранована) шафа з обладнанням КНЕДП, та робочих приміщеннях КНЕДП.

8.9.1.2. Приміщення відповідають вимогам техніки безпеки та протипожежної безпеки, комплектуються необхідними засобами енергозабезпечення, охоронної та протипожежної сигналізації, відеоспостереження (за необхідності), допоміжними технічними засобами (у робочому приміщенні КНЕДП – механічний (електронний) замок; у кімнаті реєстрації КНЕДП – механічний (електронний) замок; у спеціальному приміщенні КНЕДП: перші двері – механічний замок, другі двері – спеціальний замок із запором, системами життєзабезпечення (кондиціонерами).

8.9.1.3. Спеціальне приміщення КНЕДП відповідає вимогам до спеціальних приміщень, за виключенням вимог щодо захисту від витоку та деструктивного впливу зовнішніх електромагнітних полів, а ПТК, який використовується для обслуговування сертифікатів користувачів, має експертний висновок в галузі криптографічного захисту інформації та відповідає вимогам нормативних документів в сфері технічного захисту інформації стосовно створення комплексної системи захисту інформації.

8.9.1.4. У спеціальному приміщенні КНЕДП розміщені:

- захищена (екранована) шафа, в якій розміщується обладнання КНЕДП і яка забезпечує виконання вимог щодо захисту від витоку та деструктивного впливу зовнішніх електромагнітних полів;

8.9.1.5. Захищена (екранована) шафа має спеціальний замок із запором, ключі від якого знаходяться у системного адміністратора (дублікат ключа зберігається в сейфі начальника КНЕДП) та забезпечує можливість її опломбування. Дублікат ключа в опломбованому тубусі також знаходиться у відповідального чергового.

8.9.2 Пропускний і внутрішній режим

Пропускний і внутрішній режими визначаються внутрішніми інструкціями і передбачають порядок допуску співробітників і представників інших організацій на територію КНЕДП, порядок внесення і винесення матеріальних цінностей, а також виконання особами, що перебувають на території КНЕДП, встановлених вимог режиму й розпорядку робочого дня.

Відповідальність за організацію охорони, стан перепускного й внутрішнього режиму КНЕДП в цілому покладається на службу захисту інформації.

Загальне керівництво і контроль за організацією охорони, станом перепускного й внутрішнього режиму здійснює начальник служби захисту інформації КНЕДП.

8.9.3 Механізми контролю доступу до спеціального приміщення КНЕДП та приміщень з обмеженим доступом де розміщений ПТК КНЕДП (далі – ЦОД).

8.9.3.1. Допуск до ЦОД у супроводі відповідальної особи за експлуатацію ЦОД (або іншої уповноваженої особи) та приміщень з обмеженим доступом у режимі штатної роботи КНЕДП мають:

- керівник (начальник) КНЕДП;
- адміністратор безпеки та аудиту;
- системний адміністратор;
- адміністратор сертифікації.

8.9.3.2. Якщо КНЕДП знаходиться у режимі штатної роботи, допуск до ЦОД та приміщень з обмеженим доступом КНЕДП дозволений тільки в супроводі посадових осіб КНЕДП.

8.9.3.3. Допуск до ЦОД та приміщень з обмеженим доступом КНЕДП інших осіб, окрім визначених вище, може здійснюватися коли виконуються усі наступні умови:

- відвідування здійснюється за погодженням керівника (начальника) КНЕДП;
- склад відвідувачів, час відвідування та план робіт, що будуть виконуватися у спеціальному приміщенні КНЕДП відвідувачами задокументовані та узгоджені з адміністратором безпеки та аудиту;
- протягом усього часу знаходження відвідувачів у спеціальному приміщенні КНЕДП дії відвідувачів контролюються адміністратором безпеки та аудиту;

8.9.3.4. Факти допуску до ЦОД та приміщень з обмеженим доступом інших осіб, окрім персоналу КНЕДП, повинні бути запротокольовані (з зазначенням мети і часу відвідування, складу відвідувачів, а також їхніх ідентифікаційних даних) та засвідчені підписом адміністратора безпеки та аудиту або начальника КНЕДП.

8.10 Процедурний контроль (система дисциплінарних стягнень за недотримання працівниками КНЕДП своїх обов’язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації КНЕДП та документації на комплексну систему захисту інформації в межах організації з урахуванням режиму роботи КНЕДП).

Порушення (невиконання) положень цього Регламенту може призвести до кримінальної, цивільної або адміністративної відповідальності згідно з чинним законодавством України у вигляді позбавлення волі або штрафу, зобов’язання з відшкодування нанесених збитків, іншої дисциплінарної відповідальності.

8.11 Порядок ведення журналів аудиту подій

8.11.1 Типи подій, що фіксуються у журналах аудиту подій

ПТК КНЕДП налаштований на реєстрацію наступних подій:

– спроби створення, знищення, встановлення паролів, зміни прав доступу в інформаційно-телекомунікаційній системі;

– заміни програмного забезпечення, технічних засобів інформаційно-телекомунікаційної системи;

– технічне обслуговування інформаційно-телекомунікаційної системи;

– генерація, використання, знищення особистих ключів КНЕДП;

– формування, блокування, скасування та поновлення сертифікатів відкритих ключів, формування списків відкликаних сертифікатів відкритих ключів;

– спроби несанкціонованого доступу до інформаційно-телекомунікаційної системи;

– надання доступу персоналу до інформаційно-телекомунікаційної системи;

– збої в роботі інформаційно-телекомунікаційної системи;

– інші події, необхідні для збору доказів.

Параметри реєстрації подій в ПТК КНЕДП (в електронній або паперовій формі):

– дата, час, тип події, результат (успішність/неуспішність) події;

– ідентифікатор користувача (процесу), що ініціював подію.

Записи подій у журналах аудиту подій в паперовій формі підписуються адміністратором безпеки та аудиту.

8.11.2 Частота перегляду журналів аудиту подій

Журнали аудиту подій, що ведуться в ПТК КНЕДП, переглядаються адміністратором безпеки та аудиту періодично, але не рідше одного разу на добу з метою виявлення сукупності подій (серед зареєстрованих у журналі аудиту), які свідчать про ситуацію, яка призвела або може призвести до порушення безпеки експлуатації комплексу.

Також під час перегляду журналів аудиту подій вивчаються зафіксовані події та перевіряється наявність несанкціонованої модифікації.

8.11.3 Строки зберігання журналів аудиту подій

Журнали аудиту подій, що ведуться в ПТК КНЕДП, зберігаються протягом 5 років, після чого забезпечується їх передача на архівне зберігання.

8.11.4 Порядок захисту та резервного копіювання журналів аудиту подій, сертифікатів відкритих ключів, списків відкликаних сертифікатів

Резервні копії журналів аудиту подій, сертифікатів відкритих ключів, списків відкликаних сертифікатів на з’ємних носіях зберігаються в окремому приміщенні із забезпеченням їх захисту від несанкціонованого доступу.

Резервне копіювання журналів аудиту здійснюється раз на добу (на резервний сервер КНЕДП), резервне копіювання журналів аудиту на з’ємні носії здійснюється раз на тиждень.

Резервування здійснюється системним адміністратором відповідними засобами, що входять до складу операційної системи персонального

комп'ютера, системи керування базами даних та засобами ПТК КНЕДП, під контролем та за участю адміністратора безпеки та аудиту. Факти проведення резервування у КНЕДП протоколюються (за період) та засвідчуються підписами відповідальних осіб.

Управління доступом до резервних копій журналів аудиту та контроль за їх зберіганням та застосуванням здійснює адміністратор безпеки та аудиту.

8.11.5 Перелік посад, що можуть здійснювати перегляд журналів аудиту

Перегляд журналів аудиту, що ведуться в ПТК КНЕДП, дозволяється здійснювати лише керівнику (начальнику) КНЕДП та адміністратору безпеки та аудиту.

8.12 Порядок ведення архівів КНЕДП (із зазначенням видів документів та даних, що підлягають архівуванню, строків зберігання архівів, механізму та порядку зберігання і захисту архівів)

8.12.1 Типи документів та даних, що підлягають архівуванню

Архівному зберіганню підлягають наступні документи КНЕДП:

- сертифікати КНЕДП, відповідальних осіб КНЕДП та користувачів (чинні, скасовані, блоковані);
- реєстр відповідальних осіб КНЕДП та користувачів;
- копії і оригінали документів на папері та/або в електронній формі, що подані заявниками (користувачами) під час реєстрації (визначені у пунктах 8.6.7 – 8.6.9 та 10.9), формування, зміни статусу сертифіката, зміни даних користувачів;
- СВС;
- журнали аудиту та документи КНЕДП, у тому числі протоколи роботи ПТК КНЕДП.

8.12.2 Строки зберігання архівів

Документи КНЕДП на паперових носіях, що підлягають архівному зберіганню, зберігаються протягом строків, визначених законодавством у сфері архівної справи.

Сертифікати відкритих ключів КНЕДП, сертифікати відкритих ключів посадових осіб КНЕДП та сертифікати ключів користувачів, а також списки відкликаних сертифікатів зберігаються безстроково.

8.12.3 Механізми та порядок зберігання, захисту та знищення архівних документів

Документи КНЕДП на паперових носіях, а також, сертифікати відкритих ключів користувачів, зберігаються в порядку, встановленому законодавством України у сфері архівної справи.

Архівні документи в електронному вигляді зберігаються на з'ємних носіях із забезпеченням їх захисту від несанкціонованого доступу.

Знищення архівних документів здійснюється комісією, до складу якої входять керівник (начальник) КНЕДП, адміністратор сертифікації, адміністратор безпеки та аудиту. Після завершення процедури знищення архівних документів складається відповідний акт, який затверджує начальник КНЕДП.

8.12.4 Умови надання архівної інформації

КНЕДП надає доступ до необхідного сертифіката та пов'язаних з ним СВС з архівних записів КНЕДП за запитом заявників у строки, установлені законодавством України для відповідей на звернення громадян.

8.13 Процес, порядок та умови генерації пар ключів КНЕДП та користувачів

8.13.1 Порядок генерації ключів КНЕДП

Генерація ключів КНЕДП здійснюється у спеціальному приміщенні, що унеможливлює витік відомостей про зміст особистого ключа за рахунок побічних електромагнітних випромінювань та наведень.

Перед генерацією ключів КНЕДП усі відповідні засоби ПТК КНЕДП повинні бути встановлені та пройти тестування в установленому порядку.

Генерація ключів КНЕДП, введення даних, необхідних для створення запиту на формування сертифіката відкритого ключа КНЕДП, здійснюється адміністратором сертифікації у присутності керівника (начальника) КНЕДП та під контролем адміністратора безпеки та аудиту.

Відразу після генерації ключів КНЕДП автоматично створюється (у електронному вигляді) запит на формування сертифіката відкритого ключа КНЕДП, що містить дані (в тому числі, значення відкритого ключа КНЕДП), підписані особистим ключем КНЕДП, необхідні для формування центральним засвідчувальним органом (далі – ЦЗО) сертифіката КНЕДП. Далі цей запит використовується при підготовці документів для сертифікації відкритого ключа КНЕДП в ЦЗО.

Генерація, зберігання, використання ключів КНЕДП здійснюється виключно у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу.

Резервні копії ключів КНЕДП зберігаються у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу.

Після формування сертифікату відкритого ключа КНЕДП він публікується на електронному інформаційному ресурсі КНЕДП.

Після закінчення строку дії сертифіката відкритого ключа КНЕДП особистий ключ КНЕДП та всі його резервні копії знищуються способом, що унеможливлюють їх відновлення.

Адміністратор сертифікації під контролем адміністратора безпеки та аудиту вводить значення коду доступу до особистого ключа таким чином, щоб ніхто не мав можливості з ним ознайомитися.

Код доступу до особистого ключа КНЕДП, повинен бути відомий лише адміністратору сертифікації.

Адміністратор сертифікації записує (таким чином, щоб не допустити ознайомлення з ним інших осіб) на аркуші паперу значення коду доступу до особистого ключа КНЕДП, вміщує цей аркуш в непрозорий конверт, надписує

його, опечатує конверт разом з адміністратором безпеки та аудиту і передає на зберігання керівнику (начальнику) КНЕДП.

Не менше ніж за один календарний рік до закінчення строку дії поточного особистого ключа КНЕДП переходить на застосування нового особистого ключа КНЕДП завчасно згенерованого та сертифікованого в ЦЗО.

8.13.2 Порядок захисту та доступу до ключів КНЕДП

Ключі КНЕДП зберігаються виключно у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу.

Для застосування ключів КНЕДП необхідно ввести коди доступу до нього.

8.13.3 Порядок та умови генерації пар ключів користувачів

Відповідальні особи КНЕДП забезпечують користувачів засобами КЕП та надають йому допомогу під час генерування ключів у разі потреби.

8.13.4 Місце генерації ключів користувачів

Відкритий та особистий ключі користувача можуть бути згенеровані:

- на робочому місці користувача;
- на робочій станції адміністратора реєстрації.

8.13.5 Запити на формування сертифікату

Запит на формування сертифікату користувача може бути двох видів:

- у форматі PKCS#10;
- у форматі PKCS#7 з накладеним КЕП з використанням чинного особистого ключа користувача.

8.13.6 Зберігання особистого ключа та відповідальність

Згенерований особистий ключ користувача захищається паролем. Користувач несе відповідальність за забезпечення конфіденційності та цілісності свого особистого ключа.

8.14 Процедури отримання користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги КНЕДП

Особистий ключ генерується заявником засобами кваліфікованого електронного підпису чи печатки. Користувач власноручно вводить значення коду доступу до носія особистого ключа.

8.15 Механізм надання відкритого ключа користувача КНЕДП для формування кваліфікованого сертифіката відкритого ключа

Відкритий і особистий ключі користувача генеруються з використанням робочої станції адміністратора реєстрації або з робочого місця користувача (заявника) виключно з використанням засобів кваліфікованого електронного підпису чи печатки.

При генерації ключів створюється особистий ключ та запит на формування сертифіката ключа. Запит на формування сертифіката ключа, що передається на сертифікацію до КНЕДП, є самопідписаним запитом формату PKCS#10, який засвідчується КЕП за допомогою особистого ключа заявника (користувача).

Запит може подавати заявник, що пройшов процедуру реєстрації, підписувач (у разі позапланової заміни ключів).

Під час обробки запиту на формування сертифіката ключа здійснюється перевірка належності особистого ключа користувача відкритому ключу, який міститься у запиті. Перевірка здійснюється з використанням програмного забезпечення ПТК КНЕДП автоматично, шляхом перевірки КЕП, накладеного на запит на формування сертифіката ключа, з використанням відкритого ключа, що міститься у запиті. Формування сертифіката ключа можливе лише за умов успішної перевірки.

8.16 Порядок захисту та доступу до особистого ключа КНЕДП

Зберігання та використання ключів КНЕДП здійснюється виключно у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу.

Для застосування особистого ключа КНЕДП необхідно ввести код доступу до нього.

Особистий ключ КНЕДП застосовується лише у захищеній (екранованій) шафі в спеціальному приміщенні КНЕДП двома посадовими особами КНЕДП: адміністратором сертифікації в присутності адміністратором безпеки та аудиту.

Запечатаний та підписаний конверт із значенням коду доступу до особистого ключа КНЕДП, опечатаний адміністратором сертифікації та адміністратором безпеки аудиту, зберігається у сейфі керівника (начальника) КНЕДП.

8.17 Порядок та умови резервного копіювання особистого ключа КНЕДП, збереження, доступу та використання резервної копії

Резервне копіювання особистого ключа КНЕДП здійснюється виключно у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними або апаратними пристроями, що забезпечують захист записаних даних від несанкціонованого доступу

Резервна копія особистого ключа КНЕДП може бути застосована лише за погодженням керівника (начальника) КНЕДП та лише за умов, коли основний особистий ключ КНЕДП було знищено з причин, не пов’язаних з його компрометацією.

Застосування резервної копії особистого ключа КНЕДП здійснюється у такому ж порядку, як і використання особистого ключа КНЕДП. Про факти використання резервної копії особистого ключа КНЕДП повинен бути поінформований адміністратор безпеки.

Запечатаний тубус (контейнер), із носієм, що містить резервну копію особистого ключа КНЕДП, опечатаний адміністратором сертифікації, зберігається у сейфі начальника КНЕДП.

Запечатаний та надписаний конверт із значенням кодів доступу до носія, що містить резервну копію особистого ключа КНЕДП, опечатаний адміністратором сертифікації, та адміністратором безпеки та аудиту, зберігається у сейфі начальника КНЕДП.

9. ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

9.1 Процес подання запиту на формування кваліфікованого сертифіката відкритого ключа (перелік суб'єктів, уповноважених подавати запит на формування кваліфікованого сертифіката відкритого ключа, порядок подачі та оброблення такого запиту, строки оброблення запиту на формування кваліфікованого сертифіката відкритого ключа)

9.1.1 Перелік суб'єктів, які можуть подавати документи на формування сертифіката відкритого ключа

Документи на формування сертифіката відкритого ключа можуть подати наступні заявники:

- фізичні особи, що бажають отримати сертифікат відкритого ключа;
- юридичні особи (фізичні особи – підприємці), що бажають отримати сертифікат відкритого ключа, в особі їх посадових осіб;
- фізичні особи – власники електронних пенсійних посвідчень.

9.1.2 КНЕДП здійснює формування сертифікатів користувачів у такому порядку

Заявник під час проведення реєстрації в КНЕДП подає запит на формування сертифікату користувача, згенерований зі свого робочого місця, або генерує запит на формування сертифікату користувача в КНЕДП на робочій станції адміністратора реєстрації.

Адміністратор сертифікації з використанням робочої станції адміністратора сертифікації здійснює перевірку КЕП на засвідченому запиті на формування сертифіката відкритого ключа (така перевірка здійснюється автоматично прикладним програмним забезпеченням робочої станції адміністратора сертифікації). В разі встановлення відповідності КЕП адміністратор сертифікації формує сертифікат відкритого ключа КЕП з використанням особистого ключа КНЕДП.

Запит на формування сертифіката обробляється в КНЕДП протягом доби з моменту його надходження.

Також, під час формування сертифіката користувача КНЕДП присвоює унікальний реєстраційний номер сертифікату та перевіряє унікальність відкритого ключа користувача в реєстрі чинних, блокованих та скасованих сертифікатів. Одночасно, КНЕДП забезпечує унікальність розпізнавального імені користувача в межах КНЕДП.

Процедура встановлення належності користувача особистого ключа та його відповідність відкритому ключу здійснюється шляхом перевірки КЕП у запиті на формування сертифікату користувача. Сертифікат користувача формується лише в разі підтвердження КЕП.

9.1.3 Порядок повторного формування сертифіката відкритого ключа користувача після закінчення строку обслуговування сертифіката відкритого ключа

Процедура повторного формування сертифіката відкритого ключа користувача після закінчення строку обслуговування його сертифікату ключа ідентична процедурі первинного формування сертифіката відкритого ключа.

9.2 Порядок надання сформованого кваліфікованого сертифіката

відкритого ключа користувачу.

Сформований КНЕДП сертифікат, за бажанням користувача адміністратор реєстрації записує на носій ключової інформації та передає його користувачу;

Після отримання сертифікату відкритого ключа користувач повинен перевірити достовірність даних, що містяться в ньому. У разі виявлення розбіжностей між даними, що подавались для формування сертифікату відкритого ключа, та даними, що містяться у сертифікаті, користувач повідомляє про це КНЕДП, який вживає заходи щодо скасування сертифікату та формування нового з актуальними даними.

У разі, якщо розбіжностей не виявлено, користувач визнає свої сертифікати відкритих ключів шляхом підписання акту прийому-передачі наданих послуг. З цього моменту користувача вважається власником сертифіката відкритого ключа та може виступати суб'єктом правових відносин у сфері надання електронних довірчих послуг.

9.3 Порядок та умови публікації сформованого кваліфікованого сертифіката відкритого ключа користувача на офіційному веб-сайті КНЕДП.

В разі, якщо при формуванні сертифіката відкритого ключа користувача він погодився на його публікацією, сформований сертифікат відкритого ключа автоматично стане доступним за протоколами HTTPS.

9.4 Умови використання кваліфікованого сертифіката відкритого ключа користувача та його особистого ключа (попередження про можливі наслідки неправильного використання кваліфікованого сертифіката відкритого ключа та особистого ключа).

9.4.1 Відповідальність користувача – власника сертифіката відкритого ключа під час використання особистого ключа та сертифіката відкритого ключа

Заявник (юридична особа) несе відповідальність за організацію, а користувач (посадова особа заявника) або користувач (фізична особа) за безпосереднє надійне збереження особистого ключа та носія ключової інформації, на якому він знаходиться, а також значення коду доступу до цього носія.

Користувач несе відповідальність за розповсюдження власного сертифікату відкритого ключа (якщо користувач не дав згоду на його публікацію в КНЕДП). В цьому випадку, користувач повинен надавати сертифікат всім особам, з якими він вступає у правові відносини у сфері електронних довірчих послуг.

9.4.2 Відповідальність користувачів під час використання сертифіката відкритого ключа

Користувачі несуть відповідальність за вільне (безконтрольне) розповсюдження сертифікатів відкритих ключів інших осіб – суб'єктів правових відносин у сфері електронних довірчих послуг. Користувачі повинні усвідомлювати, що сертифікат відкритого ключа містить персональні дані цих осіб та його розповсюдження без згоди власника призведе до

неконтрольованого поширення зазначених відомостей, що може нанести цій особі моральні або матеріальні збитки.

9.5 Процедура подачі запиту на формування кваліфікованого сертифіката відкритого ключа для користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований КНЕДП.

Запит може подавати заявник, що пройшов процедуру реєстрації, підписувач (у разі позапланової заміни ключів).

В разі, якщо користувач має чинний сертифікат відкритого ключа термін дії якого закінчується та ідентифікаційні дані якого залишились незмінними, він може отримати новий сертифікат відкритого ключа за визначеною нижче процедурою для отримання сертифікату відкритого ключа.

Користувач заповнює заяву на формування сертифіката користувача в електронному вигляді, робить якісні скан-копії (з роздільною здатністю не менше 150 dpi) решти документів, визначених у розділі 8 цього Регламенту та підписує і завіряє їх встановленим чином за допомогою свого особистого ключа (до закінчення строку його чинності) і засвідчує електронною печаткою організації (в разі наявності).

Після цього повний пакет документів передається для розгляду до КНЕДП.

9.6 Обставини скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа; перелік суб'єктів, уповноважених здійснювати запит на скасування (блокування та поновлення) кваліфікованого сертифіката відкритого ключа; процедура подання запиту на скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа; час оброблення запиту на скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа; частота формування списку відкликаних сертифікатів та строки його дії; можливість та умови надання інформації про статус кваліфікованого сертифіката відкритого ключа у режимі реального часу)

9.6.1 Обставини скасування (блокування, поновлення) сертифіката відкритого ключа.

9.6.1.1. КНЕДП скасовує сертифікат відкритого ключа користувача у разі:

1) подання користувачем заяви про скасування виданого йому кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи- користувача;

2) надходження до КНЕДП документа, що підтверджує:

- смерть фізичної особи - користувача;
- припинення діяльності створювача електронної печатки;
- зміни ідентифікаційних даних користувача;
- факт державної реєстрації припинення підприємницької діяльності фізичної особи - підприємця чи припинення діяльності в установленому законодавством порядку юридичної особи;
- надання користувач недостовірних ідентифікаційних даних під час формування його кваліфікованого сертифіката відкритого ключа;

- факт компрометації особистого ключа користувача, виявлений самостійно користувачем або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;

- набрання законної сили рішенням суду про скасування кваліфікованого сертифіката відкритого ключа, оголошення користувача померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності, визнання користувача електронних довірчих послуг банкрутом.

КНЕДП автоматично скасовує сертифікат при закінченні строку його чинності.

До подій, пов'язаних з компрометацією ключів користувачів, відносяться наступні:

Будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа, зокрема:

- втрата носіїв, на які записані особисті ключі;
- втрата носіїв, на які записані особисті ключі, з наступним виявленням;
- звільнення співробітників, що мали особисті ключі;
- порушення правил зберігання особистих ключів;
- виникнення підозр на несанкціоноване застосування особистого ключа;
- втрату контролю щодо особистого ключа через компрометацію коду доступу до носія особистого ключа;
- випадки, коли не можна вірогідно встановити, що відбулося з носіями, що містять ключову інформацію (у тому числі, випадки, коли носій вийшов з ладу й доказово не спростована можливість того, що даний факт відбувся в результаті несанкціонованих дій зловмисника).

У випадку компрометації ключа користувач зобов’язаний терміново сповістити про цей факт КНЕДП та виконати дії згідно пункту 9.6.3. Регламенту.

До зміни ідентифікаційних даних користувача належать:

- переведення на іншу посаду або звільнення з роботи власника сертифіката відкритого ключа (для сертифікатів ключів юридичних осіб/посадових осіб);
- зміна прізвища;
- зміна місця прописки/реєстрації в частині, що вказана в реквізитах власника сертифіката відкритого ключа;
- виявлення помилок у реквізитах тощо.

Зміна зовнішніх обставин, які навіть при збереженні реквізитів власника сертифіката відкритого ключа змінюють його статус, що впливає на правомочність КЕП, зокрема, зміна положення про посаду, що призводить до того, що зазначені в сертифікаті відкритого ключа повноваження більше йому не належать (в тому числі втрата права підпису звітності, керування банківським рахунком тощо) потребує скасування сертифіката.

За виникнення будь-яких вищезазначених причин та обставин користувач зобов’язаний невідкладно заблокувати сертифікат відкритого ключа та протягом терміну дії блокування виконати операції зі скасування сертифіката відкритого ключа згідно пункту 9.6.6.3. Регламенту.

9.6.1.2. КНЕДП блокує сертифікат відкритого ключа користувача у разі:

- подання користувачем заяви про блокування виданого йому кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи- користувача;
- повідомлення користувачем або контролюючим органом про підозру в компрометації особистого ключа користувача;
- набрання законної сили рішенням суду про блокування кваліфікованого сертифіката відкритого ключа;
- порушення користувачем істотних умов договору про надання кваліфікованих електронних довірчих послуг.

9.6.1.3. Блокований сертифікат відкритого ключа поновлюється у разі:

- подання користувачем заяви про поновлення його заблокованого кваліфікованого сертифіката відкритого ключа (якщо блокування здійснено на підставі заяви про блокування кваліфікованого сертифіката відкритого ключа);
- повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа користувачем або контролюючим органом, який раніше повідомив про цю підозру;
- надходження до КНЕДП повідомлення про прийняття рішення суду про поновлення кваліфікованого сертифіката відкритого ключа, що набрало законної сили.

9.6.2 Перелік суб’єктів, уповноважених подавати заяву на скасування (блокування, поновлення) сертифіката відкритого ключа

Уповноваженими на подання заяви на скасування (блокування, поновлення) сертифіката відкритого ключа є користувачі та заявники (щодо користувачів, що відносяться до заявника).

9.6.3 Процедура подання заяви на скасування (блокування, поновлення) сертифіката відкритого ключа

9.6.3.1 Загальні відомості щодо скасування (блокування, поновлення) сертифіката відкритого ключа

Блокування тимчасово припиняє дію сертифіката відкритого ключа. Після блокування сертифіката користувач зобов’язаний або поновити сертифікат, або виконати скасування сертифікату.

Кваліфікований сертифікат відкритого ключа, статус якого змінено на заблокований, у період блокування не використовується.

Скасування припиняє дію сертифікату. Скасовані сертифікати поновленню не підлягають.

Поновлення чинності сертифікату ключа можливе лише для сертифікатів, що заблоковані і термін чинності сертифіката не скінчився.

9.6.3.2. Порядок блокування сертифіката відкритого ключа

Для здійснення блокування сертифіката користувач подає заяву на блокування до КНЕДП.

Блокування сертифіката здійснюється КНЕДП на підставі заяви, що надходить установленим порядком в КНЕДП в усній, паперовій формі чи у вигляді електронного документа.

Кваліфікований сертифікат відкритого ключа вважається заблокованим з моменту зміни КНЕДП статусу кваліфікованого сертифіката відкритого ключа на заблокований.

Блокування сертифіката здійснюється протягом двох годин з моменту настання події, зазначеної у п. 9.6.1.2 Регламенту.

9.6.3.2.1. Блокування сертифіката за заявою в усній формі

Заява на блокування в усній формі подається в КНЕДП за телефоном.

Користувач повинен повідомити адміністратору реєстрації КНЕДП наступну інформацію:

- ідентифікаційні дані власника сертифікату відкритого ключа;
- серійний номер сертифіката, що блокується (якщо користувач має більш, ніж один діючий сертифікат);
- парольну фразу (слово з парольної фрази) голосової автентифікації.

Заява в усній формі приймається тільки у випадку позитивної автентифікації
(збігу даних користувача та парольної фрази, переданих в заяві, з інформацією, що наявною в реєстрі користувачів КНЕДП).

Приймання і обробка заяви в усній формі здійснюється цілодобово. Обробка заяви в усній формі на блокування сертифіката та інформування користувача здійснюється безпосередньо після приймання заяви протягом двох годин.

Якщо блокування сертифіката відкритого ключа користувача здійснюється в усній формі у неробочий час (пн-чт з 18.00 до 9.00, п’ятниця з 17.00) або у вихідні, святкові та неробочі дні, адміністратор (оператор) реєстрації протягом 2 (двох) годин з моменту надходження телефонного запиту від користувача телефонує користувачу, здійснює його автентифікацію та отримує усне підтвердження щодо правильності поданого ним запиту. Подальша обробка запиту відбувається згідно вищеописаного порядку.

9.6.3.2.2. Блокування сертифіката за заявою в паперовій формі

Заява в паперовій формі подається в КНЕДП за встановленою формою, яку можливо отримати з електронного інформаційного ресурсу КНЕДП.

Заява на блокування сертифіката засвідчується відповідно до п. 8.7 Регламенту.

Подача заяви на блокування сертифіката в КНЕДП та її розгляд здійснюється тільки в робочий час, відповідно до розпорядку роботи КНЕДП.

9.6.3.2.3. Блокування сертифіката за заявою у електронній формі

Електронна заява подається до КНЕДП за встановленою формою та засвідчується користувачем за допомогою свого особистого ключа (до закінчення строку його чинності) і електронною печаткою організації (в разі наявності). Заяви приймаються на електронну адресу csk@uss.gov.ua.

Подача заяви на блокування сертифіката в КНЕДП та її розгляд здійснюється тільки в робочий час, відповідно до розкладу роботи КНЕДП.

9.6.3.3. Порядок скасування сертифіката відкритого ключа

Для скасування сертифіката користувач подає заяву на скасування до КНЕДП.

Скасування сертифіката здійснюється КНЕДП на підставі заяви, що надходить встановленим порядком в КНЕДП в паперовій або електронній формі.

Заява на скасування сертифіката в паперовій формі подається в КНЕДП за відповідною формою, яка доступна на інформаційному ресурсі КНЕДП.

Електронна заява подається до КНЕДП за встановленою формою та засвідчується користувачем за допомогою свого особистого ключа (до закінчення строку його чинності) і електронною печаткою організації (в разі наявності). Заяви приймаються на електронну адресу: csk@uss.gov.ua цілодобово.

Подача до КНЕДП заяви на скасування сертифіката в паперовій формі та її розгляд здійснюється тільки в робочий час, відповідно до розпорядку роботи КНЕДП.

Скасування сертифіката здійснюється протягом двох годин з моменту настання події, зазначеної у п. 9.6.1.1 Регламенту.

Кваліфікований сертифікат відкритого ключа вважається скасованим з моменту зміни КНЕДП статусу кваліфікованого сертифіката відкритого ключа на скасований.

9.6.3.4. Порядок поновлення сертифіката відкритого ключа

Поновлення чинності сертифікату ключа можливе лише для сертифікатів, що заблоковані і термін чинності сертифіката не скінчився. Скасовані сертифікати поновленню не підлягають.

Поновлення чинності сертифіката здійснюється КНЕДП на підставі заяви, що надходить встановленим порядком в КНЕДП в паперовій формі, разом з новою парольною фразою.

Заява на поновлення сертифіката подається в КНЕДП за відповідною формою, яка доступна на інформаційному ресурсі КНЕДП.

Приймання заяв на поновлення сертифіката виконується КНЕДП цілодобово, а ВПР тільки в робочий час (відповідно до розпорядку роботи).

Поновлення сертифіката здійснюється протягом двох годин з моменту настання події, зазначеної у п. 9.6.1.3 Регламенту.

Кваліфікований сертифікат відкритого ключа вважається поновленим з моменту зміни КНЕДП статусу кваліфікованого сертифіката відкритого ключа на поновлений.

9.6.4 Час оброблення запитів на скасування (блокування, поновлення) сертифіката відкритого ключа

Приймання і обробка запиту на блокування сертифіката в усній формі здійснюється цілодобово.

Обробка запиту на скасування (блокування, поновлення) сертифіката в паперовій формі здійснюється протягом двох годин з моменту отримання такого запиту.

9.7 Строк закінчення дії кваліфікованого сертифіката відкритого ключа користувача

Статус сертифіката змінюється автоматично на «нечинний» при закінченні строку чинності сертифіката відкритого ключа. Така зміна статусу не потребує переформування списку відкликаних сертифікатів.

Термін дії для особистих ключів дорівнює терміну дії відповідних їм відкритих ключів. Термін дії відкритих ключів визначається терміном чинності сертифікатів відкритих ключів.

Терміни чинності сертифікатів відкритих ключів:

- сертифікат відкритого ключа КНЕДП – не більше ніж 5 років;
- сертифікат відкритого ключа послуг фіксування часу, послуг визначення статусу сертифікату ключа в режимі реального часу за протоколом OCSP, протокол управління сертифікатами TCP – не більше ніж 5 роки;
- сертифікат відкритого ключа посадової особи КНЕДП – не більше ніж 2 роки;
- сертифікат відкритого ключа користувача – не більше ніж 2 роки.

Проміжки часу, протягом яких є чинними ключі посадової особи КНЕДП та ключі, що застосовуються при наданні послуг фіксування часу, повинні цілком знаходитися у проміжку часу, протягом якого є чинним ключ КНЕДП.