

ПОГОДЖЕНО

Заступник Міністра цифрової
трансформації України



Валерія КОВАЛЬ

2026 року

ЗАТВЕРДЖУЮ

Генеральний прокурор



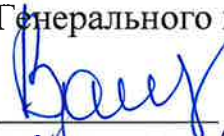
Руслан КРАВЧЕНКО

«26» червня 2026 року

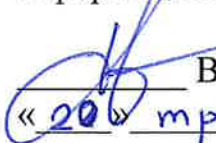
РЕГЛАМЕНТ РОБОТИ КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ ОРГАНІВ ПРОКУРАТУРИ УКРАЇНИ

(оновлена редакція)

Перший заступник
Генерального прокурора

 Марія ВДОВИЧЕНКО
«21» травня 2026 року

Керівник Кваліфікованого надавача
електронних довірчих послуг органів
прокуратури України,
заступник начальника Департаменту
інформаційних технологій

 Володимир КУПЕЦЬКИЙ
«20» травня 2026 року

ЗМІСТ

ЗАГАЛЬНІ ПОЛОЖЕННЯ.....	5
ПЕРЕЛІК СКОРОЧЕНЬ	5
ВИЗНАЧЕННЯ ТЕРМІНІВ	5
СУБ'ЄКТИ ВІДНОСИН.....	6
СТАТУС РЕГЛАМЕНТУ РОБОТИ.....	7
ПОРЯДОК ЗАТВЕРДЖЕННЯ І ВНЕСЕННЯ ЗМІН ТА ДОПОВНЕНЬ ДО РЕГЛАМЕНТУ	8
1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО НАДАВАЧА	9
1.1. Ідентифікаційні дані КНЕДП.....	9
1.2. СФЕРА ТА ПІДСТАВИ ДІЯЛЬНОСТІ КНЕДП	9
2. ПЕРЕЛІК КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, НАДАННЯ ЯКИХ ЗАБЕЗПЕЧУЄ НАДАВАЧ	10
3. ПЕРЕЛІК ПОСАД НАЙМАНИХ ПРАЦІВНИКІВ, ОБОВ'ЯЗКИ ЯКИХ БЕЗПОСЕРЕДНЬО ПОВ'ЯЗАНІ З НАДАННЯМ КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, ТА ФУНКЦІЇ ТАКИХ ПРАЦІВНИКІВ.....	12
3.1. ОРГАНІЗАЦІЙНА СТРУКТУРА КНЕДП.....	12
3.1.1. Керівник КНЕДП.....	12
3.1.2. Заступник керівника КНЕДП – адміністратор сертифікації та адміністратор сертифікації	13
3.1.3. Адміністратор безпеки.....	14
3.1.4. Аудитор системи.....	14
3.1.5. Системний адміністратор	14
3.1.6. Адміністратор реєстрації	15
3.1.7. Оператор реєстрації.....	17
3.1.8. Чергові адміністратори реєстрації КНЕДП.....	18
3.1.9. Посадові особи КНЕДП (керівник, заступник керівника – адміністратор сертифікації, адміністратор сертифікації, адміністратори безпеки, аудитор системи, адміністратори реєстрації, системний адміністратор, оператор реєстрації, чергові адміністратори реєстрації)	20
3.2. ВІДОКРЕМЛЕНІ ПУНКТИ РЕЄСТРАЦІЇ	20
4. ПОЛІТИКА СЕРТИФІКАТА ТА ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК.....	22
4.1. ПЕРЕЛІК СФЕР, В ЯКИХ ДОЗВОЛЯЄТЬСЯ ВИКОРИСТАННЯ КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ, СФОРМОВАНИХ НАДАВАЧЕМ.....	22
4.2. ОБМЕЖЕННЯ ЩОДО ВИКОРИСТАННЯ КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ, СФОРМОВАНИХ НАДАВАЧЕМ,	22
4.3. ПЕРЕЛІК ІНФОРМАЦІЇ, ЩО РОЗМІЩУЄТЬСЯ НАДАВАЧЕМ НА СВОЄМУ ОФІЦІЙНОМУ ВЕБ-САЙТІ (ІНФОРМАЦІЙНОМУ РЕСУРСІ КНЕДП)	23
4.4. ЧАС І ПОРЯДОК ПУБЛІКАЦІЇ КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ ТА СПИСКІВ ВІДКЛИКАНИХ СЕРТИФІКАТІВ	24
4.5. МЕХАНІЗМ ПІДТВЕРДЖЕННЯ ВОЛОДІННЯ ЗАЯВНИКОМ ОСОБИСТИМ КЛЮЧЕМ, ВІДПОВІДНИЙ ЯКОМУ ВІДКРИТИЙ КЛЮЧ НАДАЄТЬСЯ ДЛЯ ФОРМУВАННЯ КВАЛІФІКОВАНОГО СЕРТИФІКАТА ВІДКРИТОГО КЛЮЧА	25
4.6. УМОВИ ВСТАНОВЛЕННЯ ЗАЯВНИКА.....	25
4.6.1. Загальні положення.....	25
4.6.2. Порядок ідентифікації та реєстрації Підписувачів (Створювачів електронної печатки, Заявників).....	27
4.6.3. Процедура проведення реєстрації Заявника.....	29
4.7. МЕХАНІЗМ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ, ЯКІ МАЮТЬ ЧИННИЙ КВАЛІФІКОВАНИЙ СЕРТИФІКАТ ВІДКРИТОГО КЛЮЧА, СФОРМОВАНИЙ НАДАВАЧЕМ	30
4.8. МЕХАНІЗМ ВСТАНОВЛЕННЯ КОРИСТУВАЧІВ З ПИТАНЬ БЛОКУВАННЯ, СКАСУВАННЯ АБО ПОНОВЛЕННЯ КВАЛІФІКОВАНОГО СЕРТИФІКАТА ВІДКРИТОГО КЛЮЧА	30
4.9. ОПИС ФІЗИЧНОГО СЕРЕДОВИЩА	30
4.9.1. МЕХАНІЗМИ КОНТРОЛЮ ДОСТУПУ ДО СПЕЦІАЛЬНОГО ПРИМІЩЕННЯ.....	31
4.10. ПРОЦЕДУРНИЙ КОНТРОЛЬ	32
4.11. Порядок ведення електронних журналів аудиту подій.....	33
4.12. Порядок ведення архівів надавача	33
4.13. ПРОЦЕС, ПОРЯДОК ТА УМОВИ ГЕНЕРАЦІЇ ПАР КЛЮЧІВ НАДАВАЧА ТА КОРИСТУВАЧІВ	34
4.13.1. Порядок формування запиту на сертифікат КНЕДП.....	36

4.13.2.	Порядок використання особистого ключа КНЕДП	36
4.13.3.	Порядок планової зміни ключів КНЕДП.....	36
4.13.4.	Порядок позапланової зміни ключів КНЕДП	37
4.13.5.	Процес, порядок та умови генерації пар ключів користувачів.....	38
4.14.	Порядок захисту та доступу до особистого ключа КНЕДП	39
4.15.	Порядок та умови резервного копіювання особистого ключа надавача, збереження, доступу та використання резервної копії	39
4.16.	Умови зберігання ключів КНЕДП.....	41
4.17.	Процедури отримання користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги її надавачем	41
4.18.	Механізм надання відкритого ключа користувача надавачу для формування кваліфікованого сертифіката відкритого ключа	41
4.19.	Положення сертифікаційних практик.....	41
4.19.1.	Процес подання запиту на формування кваліфікованого сертифіката відкритого ключа Підписувача (Створювача електронної печатки).....	41
4.19.2.	Порядок формування сертифікатів та надання їх користувачу.....	44
	а) <i>Порядок первинного формування сертифіката</i>	44
	б) <i>Порядок повторного формування сертифіката</i>	45
4.19.3.	Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа користувача на офіційному веб-сайті надавача	45
4.19.4.	Умови використання кваліфікованого сертифіката відкритого ключа користувача та його особистого ключа.....	46
4.20.	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).....	46
4.20.1.	<i>Причини, за яких Підписувач (Створювач електронної печатки) зобов'язаний скасувати сертифікат</i>	47
4.20.2.	<i>Порядок блокування сертифікатів</i>	48
4.20.3.	<i>Блокування сертифіката за заявою в усній формі</i>	49
4.20.4.	<i>Блокування сертифіката за заявою в паперовій формі</i>	49
4.20.5.	<i>Блокування сертифіката за зверненням керівництва установи, до якої належить Підписувач</i> 50	
4.20.6.	<i>Блокування сертифіката за зверненням керівництва установи, до якої належить представник Створювача електронної печатки</i>	51
4.20.7.	<i>Блокування сертифіката за повідомленням контролюючого органа чи на підставі судового рішення</i> 51	
4.20.8.	<i>Порядок скасування сертифікатів</i>	52
4.20.9.	<i>Скасування сертифіката за заявою в усній формі</i>	52
4.20.10.	<i>Скасування сертифіката за заявою в паперовій формі</i>	53
4.20.11.	<i>Скасування сертифіката за зверненням керівництва установи, до якої належить Підписувач</i>	54
4.20.12.	<i>Скасування сертифіката за зверненням керівництва установи, до якої належить представник Створювача електронної печатки</i>	55
4.20.13.	<i>Скасування сертифіката за повідомленням контролюючого органа чи на підставі судового рішення</i> 56	
4.20.14.	<i>Порядок поновлення чинності сертифікатів</i>	56
4.20.15.	<i>Поновлення чинності сертифіката за заявою в усній формі</i>	57
4.20.16.	<i>Поновлення чинності сертифіката за заявою в паперовій формі</i>	57
4.20.17.	<i>Поновлення чинності сертифіката за зверненням керівництва установи, до якої належить Підписувач (Створювач електронної печатки)</i>	58
4.20.18.	<i>Поновлення чинності сертифіката за повідомленням контролюючого органа чи на підставі судового рішення</i>	58
4.21.	Порядок надання Надавачем інформації про статус сертифіката	59
4.21.1.	<i>Отримання статусу сертифіката за допомогою OCSP</i>	60
4.21.2.	<i>Отримання статусу сертифіката за допомогою CVC</i>	60

4.22. СТРОК ЗАКІНЧЕННЯ ДІ КВАЛІФІКОВАНОГО СЕРТИФІКАТА ВІДКРИТОГО КЛЮЧА ПІДПISУВАЧА (СТВОРЮВАЧА ЕЛЕКТРОННОЇ ПЕЧАТКИ).....	61
5. ОПИС ПРОЦЕДУР ТА ПРОЦЕСІВ, ЯКІ ВИКОНУЮТЬСЯ ПІД ЧАС НАДАННЯ КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, ЩО НЕ ПЕРЕДБАЧАЮТЬ ФОРМУВАННЯ ТА ОБСЛУГОВУВАННЯ КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ВІДКРИТИХ КЛЮЧІВ	62
5.1. НАДАННЯ ЗАСОБІВ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПISУ ЧИ ПЕЧАТКИ.....	62
5.2. НАДАННЯ КВАЛІФІКОВАНОЇ ЕЛЕКТРОННОЇ ДОВІРЧОЇ ПОСЛУГИ ФОРМУВАННЯ, ПЕРЕВІРКИ ТА ПІДТВЕРДЖЕННЯ КВАЛІФІКОВАНОЇ ЕЛЕКТРОННОЇ ПОЗНАЧКИ ЧАСУ	62
ПЕРЕЛІК ЗМІН ДО РЕГЛАМЕНТУ	64

Додатки:

Додаток № 1. Заява на проведення реєстрації та формування кваліфікованого сертифіката відкритого ключа електронного підпису.

Додаток № 2. Заява на проведення реєстрації та формування кваліфікованого сертифіката відкритого ключа електронної печатки.

Додаток № 3. Заява про зміну статусу кваліфікованого сертифіката відкритого ключа електронного підпису чи електронної печатки.

Загальні положення

Перелік скорочень

БД	база даних
ВПР	відокремлений пункт реєстрації
ІКС	інформаційно-комунікаційна система
ЕДП	електронні довірчі послуги
ЗКЕП	засіб кваліфікованого електронного підпису чи печатки
КЕДП	кваліфіковані електронні довірчі послуги
КЕП	кваліфікований електронний підпис/печатка
КЗІ	криптографічний захист інформації
КНЕДП	кваліфікований надавач електронних довірчих послуг
КСЗІ	комплексна система захисту інформації
ПЗ	програмне забезпечення
ПТК	програмно-технічний комплекс
СВС	список відкликаних сертифікатів
СУБД	система управління базами даних
ТЗІ	технічний захист інформації
ЦЗО	Центральний засвідчувальний орган
ЦОД	центр обробки даних

Визначення термінів

У цьому Регламенті терміни вживаються у значеннях, наведених у Законах України «Про електронні довірчі послуги» та «Про електронні документи та електронний документообіг»; Вимогах у сфері електронних довірчих послуг, Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності; Вимогах з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації, інших нормативно-правових актах у сфері електронних довірчих послуг та з питань криптографічного і технічного захисту інформації.

Суб'єкти відносин

Суб'єктами відносин, що визначаються положеннями цього Регламенту, є:

КНЕДП органів прокуратури України – підрозділ Офісу Генерального прокурора, який відповідає за надання кваліфікованих електронних довірчих послуг, забезпечує функціонування та розвиток Надавача, виконання вимог Закону України «Про електронні довірчі послуги» (далі – Закон), іншого законодавства щодо діяльності КНЕДП і у сфері захисту персональних даних та відомості про якого внесено до Довірчого списку.

Відокремлений пункт реєстрації (далі – ВПР) – підрозділ обласної прокуратури, який здійснює надання кваліфікованих електронних довірчих послуг з реєстрації та обслуговування Користувачів ЕДП на відповідній території.

Користувач кваліфікованих електронних довірчих послуг – Заявник, Підписувач, Створювач електронної печатки, інші юридичні особи (представники юридичних осіб), які отримують електронні довірчі послуги у Надавача, його відокремлених пунктів реєстрації.

Заявник – посадова особа, яка звертається до Надавача, його відокремлених пунктів реєстрації з метою формування сертифіката.

Підписувач – особа, яка на законних підставах володіє особистим ключем та від свого імені накладає кваліфікований електронний підпис під час створення електронного документа.

Підписувачами можуть бути лише працівники органів прокуратури України або посадові особи інших органів державної влади (далі – державні органи), які звернулись у встановленому Регламентом порядку до КНЕДП чи його ВПР з метою отримання електронних довірчих послуг для доступу до інформаційно-комунікаційних систем, власником/розпорядником яких є Офіс Генерального прокурора.

Створювач електронної печатки – юридична особа, яка створює електронну печатку, чи її підрозділ у визначених законодавством випадках.

Створювачами електронної печатки можуть бути органи прокуратури України або інші державні органи, які звернулись у встановленому Регламентом порядку до КНЕДП чи його ВПР з метою отримання електронних довірчих послуг для доступу до інформаційно-комунікаційних систем, власником/розпорядником яких є Офіс Генерального прокурора.

Підписувач, Створювач електронної печатки здійснює використання особистого ключа відповідно до положень цього Регламенту.

Норми цього Регламенту є обов'язковими для Підписувача, Створювача електронної печатки та КНЕДП, його ВПР з моменту подачі Підписувачем чи Створювачем електронної печатки заяви до КНЕДП, його ВПР на отримання сертифіката відкритого ключа.

Статус Регламенту роботи

Цей Регламент роботи є нормативним документом, що визначає організаційно-методичні, технічні та технологічні умови діяльності Кваліфікованого надавача електронних довірчих послуг органів прокуратури України (далі – КНЕДП або Надавач), відокремлених пунктів реєстрації під час надання кваліфікованих електронних довірчих послуг, включаючи політику сертифіката та положення сертифікаційних практик, встановлює порядок роботи та процедури КНЕДП з надання кваліфікованих електронних довірчих послуг.

Норми цього Регламенту роботи Надавача (далі – Регламент) є обов’язковими до виконання та поширюються на всіх суб’єктів відносин, які в ньому визначені. Чітке дотримання та виконання умов Регламенту для всіх сторін, що визначаються ним як суб’єкти відносин, є обов’язковим.

Будь-яка зацікавлена особа може ознайомитися з положеннями Регламенту на електронному інформаційному ресурсі, в приміщенні КНЕДП та його відокремлених пунктів.

Регламент розроблений відповідно до:

- Закону України «Про електронну ідентифікацію та електронні довірчі послуги» від 18.12.2024 № 2155-VIII;
- Закону України «Про електронні документи та електронний документообіг» від 31.12.2023 № 851-IV;
- Постанови Кабінету Міністрів України від 28 червня 2024р. № 764 «Деякі питання електронної ідентифікації та електронних довірчих послуг».
- Постанови Кабінету Міністрів України від 01.08.2023р. № 798 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності».
- Наказу Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 27.10.2020 № 687 «Про затвердження переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації». Зареєстровано в Міністерстві юстиції України 21 грудня 2020 р. за № 1272/35555.

Порядок затвердження і внесення змін та доповнень до Регламенту

Регламент затверджується Генеральним прокурором за погодженням з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України.

Внесення змін та доповнень до цього Регламенту здійснюється у порядку, встановленому для його затвердження, відповідно до чинного законодавства України.

Про внесення змін та доповнень до цього Регламенту КНЕДП повідомляє Підписувачів та інших зацікавлених осіб шляхом розміщення зазначених змін та доповнень на електронному інформаційному ресурсі КНЕДП.

Зміни та доповнення 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.

Зміни та доповнення, внесені до Регламенту у зв'язку зі зміною законодавства України, набувають чинності одночасно з набранням чинності змінами до відповідних нормативно-правових актів.

1. Загальні відомості про Надавача

1.1. Ідентифікаційні дані КНЕДП

Повне найменування юридичної особи: Офіс Генерального прокурора.

Повне найменування юридичної особи англійською мовою: General Prosecutor's Office.

Скорочене найменування юридичної особи: ОГП.

Повне найменування Надавача: Кваліфікований надавач електронних довірчих послуг органів прокуратури України.

Повне найменування Надавача англійською мовою: Qualified Trust Services Provider of the Prosecution Bodies of Ukraine.

Скорочене найменування Надавача: КНЕДП ОПУ.

Скорочене найменування Надавача англійською мовою: QTSP of the Prosecution Bodies of Ukraine.

КНЕДП ОПУ підпорядкований Департаменту інформаційних технологій і розміщується за адресою: Україна, 01011, м. Київ, вул. Різницька, 13/15.

Телефон: +38 (044) 200-75-84.

Код ЄДРПОУ: 00034051.

Електронна поштова скринька (e-mail): csk@gp.gov.ua

Електронна адреса офіційного інформаційного ресурсу (веб-сайту) Надавача: <https://ca.gp.gov.ua>

1.2. Сфера та підстави діяльності КНЕДП

КНЕДП здійснює свою діяльність у сфері надання електронних довірчих послуг органам прокуратури чи іншим органам державної влади, їх посадовим особам та працівникам, які звернулись у встановленому Регламентом порядку до КНЕДП чи його відокремлених пунктів реєстрації з метою отримання електронних довірчих послуг для доступу до інформаційно-комунікаційних систем, власником / розпорядником яких є Офіс Генерального прокурора, у тому числі інформаційної системи «Система електронного документообігу органів прокуратури України».

Діяльність КНЕДП не поширюється на відносини, що виникають під час використання інших видів електронного підпису, в тому числі переведеного у цифрову форму зображення власноручного підпису.

2. Перелік кваліфікованих електронних довірчих послуг, надання яких забезпечує надавач

Під електронними довірчими послугами розуміються послуги, які надаються для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги, зокрема надання у користування засобів КЕП, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені Законом України «Про електронну ідентифікацію та електронні довірчі послуги» від 18.12.2024 № 2155-VIII.

Перелік послуг КЕДП, що надаються КНЕДП:

1) Створення, перевірка та підтвердження кваліфікованого електронного підпису (за умови здійснення генерації особистого ключа на захищений носій) чи печатки, що включає:

- надання користувачам КЕДП засобів кваліфікованого електронного підпису чи печатки для генерації пар ключів та/або створення кваліфікованих електронних підписів чи печаток, та/або перевірки кваліфікованих електронних підписів чи печаток;
- технічну підтримку та обслуговування наданих засобів кваліфікованого електронного підпису чи печатки.

2) Формування, перевірка та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, що включає:

- створення умов для генерації пари ключів особисто Підписувачем чи Створювачем (уповноваженим представником створювача) електронної печатки за допомогою засобу кваліфікованого електронного підпису чи печатки;
- формування кваліфікованих сертифікатів електронного підпису чи печатки та видачу їх користувачу КЕДП;
- скасування, блокування та поновлення кваліфікованих сертифікатів електронного підпису чи печатки;
- перевірку та підтвердження чинності кваліфікованих сертифікатів електронного підпису чи печатки шляхом надання третім особам інформації про їхній статус;
- надання доступу до сформованих кваліфікованих сертифікатів електронних підписів та печаток за умови згоди Підписувача чи Створювача електронної печатки на публікацію кваліфікованого сертифіката електронного підпису чи печатки.

3) Формування, перевірка та підтвердження кваліфікованої електронної позначки часу, що включає:

- формування кваліфікованої електронної позначки часу;
- передачу кваліфікованої електронної позначки часу користувачеві КЕДП.

Надання вищезазначених послуг здійснюється КНЕДП відповідно до вимог законодавства у сфері електронної ідентифікації та електронних довірчих послуг та цього Регламенту.

Визнання і виконання вимог цього Регламенту користувачами КЕДП є обов'язковою умовою для надання КЕДП.

Надавач має право самостійно обирати, які саме стандарти будуть ним застосовуватися при наданні КЕДП із переліку стандартів, визначених Вимогами у сфері електронної ідентифікації та електронних довірчих послуг також стандартами в сфері електронної ідентифікації та електронних довірчих послуг.

Відповідно до статті 17 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» результати надання електронних довірчих послуг, що відповідають вимогам цього Закону, повинні визнаватися усіма користувачами таких послуг, іншими фізичними та юридичними особами.

Органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності зобов'язані забезпечити використання результатів надання кваліфікованих електронних довірчих послуг від усіх кваліфікованих надавачів електронних довірчих послуг.

3. Перелік посад найманих працівників, обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг, та функції таких працівників

3.1. Організаційна структура КНЕДП

До складу КНЕДП входять:

- керівник КНЕДП;
- заступник керівника КНЕДП – адміністратор сертифікації;
- адміністратор безпеки;
- аудитор системи;
- адміністратор сертифікації;
- адміністратори реєстрації;
- системний адміністратор;
- оператори реєстрації;
- чергові адміністратори реєстрації;
- адміністратори реєстрації ВПР.

До складу КНЕДП можуть входити й інші підрозділи, що забезпечують його роботу.

3.1.1. Керівник КНЕДП

Функції та завдання керівника КНЕДП:

- здійснює загальне керівництво діяльністю КНЕДП, забезпечує ефективне використання і збереження майна КНЕДП, організацію діловодства, виконання завдань, передбачених Регламентом КНЕДП;
- розглядає документи, що надійшли до КНЕДП, у межах компетенції підписує, затверджує та візує службову документацію;
- контролює роботу відокремлених пунктів реєстрації КНЕДП (далі – ВПР КНЕДП);
- визначає систему організаційних і технічних заходів збереження конфіденційної інформації КНЕДП та Офісу Генерального прокурора;
- подає звіти про роботу КНЕДП до центрального засвідчувального органу (далі – ЦЗО) та Державної служби спеціального зв'язку та захисту інформації України (відповідно до вимог нормативної документації);
- вживає заходів щодо підвищення ефективності роботи посадових осіб КНЕДП та ВПР КНЕДП;
- організовує впровадження нових форм і методів управління КНЕДП та ВПР КНЕДП, створення організаційних і адміністративних умов для ефективної праці у КНЕДП;
- організовує створення безпечних і сприятливих умов праці;
- у встановленому порядку звертається до державних органів, підприємств, установ, організацій незалежно від форми власності та фізичних осіб,

підписує, направляє та отримує у встановленому порядку листи, заяви, скарги, запити, відповіді на них та інші документи, що стосуються діяльності КНЕДП;

- у встановленому порядку забезпечує підготовку проєктів організаційно-розпорядчих документів з питань, що належать до компетенції КНЕДП;
- у встановленому порядку ініціює питання про необхідність застосування до посадових осіб КНЕДП заходів дисциплінарного впливу;
- за дорученням керівництва Офісу Генерального прокурора представляє в органах державної влади, громадських, наукових, міжнародних та інших організаціях Офіс Генерального прокурора з питань діяльності КНЕДП;
- вносить на розгляд керівництва Офісу Генерального прокурора або керівників самостійних структурних підрозділів пропозиції з питань, пов'язаних із діяльністю КНЕДП або його відокремлених пунктів;
- доводить до відома розробників програмно-технічного комплексу (далі – ПТК) та постачальників іншого програмного та апаратного забезпечення, що застосовується в КНЕДП, пропозиції та зауваження щодо роботи зазначених компонентів КНЕДП;
- здійснює оперативне управління майном КНЕДП;
- виконує функції адміністратора сертифікації КНЕДП.

3.1.2. Заступник керівника КНЕДП – адміністратор сертифікації та адміністратор сертифікації

Функції та завдання заступника керівника КНЕДП – адміністратора сертифікації та адміністратора сертифікації:

- бере участь у генерації пар ключів Надавача та створенні резервних копій особистих ключів Надавача;
- забезпечує зберігання особистих ключів Надавача та їх резервних копій;
- забезпечує використання особистих ключів Надавача під час формування та обслуговування кваліфікованих сертифікатів відкритих ключів Надавача та користувачів;
- перевіряє заяви про формування кваліфікованих сертифікатів відкритих ключів Надавача на відповідність вимогам Регламенту роботи Надавача;
- бере участь у знищенні особистих ключів Надавача;
- забезпечує ведення, архівування та відновлення баз даних кваліфікованих сертифікатів відкритих ключів користувачів;
- забезпечує публікацію кваліфікованих сертифікатів відкритих ключів користувачів в LDAP-каталозі та списків відкликаних сертифікатів на офіційному веб-сайті Надавача;
- забезпечує створення резервних копій кваліфікованих сертифікатів відкритих ключів користувачів;
- забезпечує зберігання кваліфікованих сертифікатів відкритих ключів користувачів, їх резервних копій, списків відкликаних сертифікатів та інших важливих ресурсів ІКС Надавача.

3.1.3. Адміністратор безпеки

Функції та завдання адміністратора безпеки:

- бере участь у генерації пар ключів Надавача та створенні резервних копій особистих ключів Надавача;
- здійснює контроль за формуванням, обслуговуванням, створенням та перевіркою резервних копій кваліфікованих сертифікатів відкритих ключів Надавача, користувачів та списків відкликаних сертифікатів;
- здійснює контроль за зберіганням особистих ключів Надавача та їх резервних копій, особистих ключів адміністраторів;
- бере участь у знищенні особистих ключів Надавача, здійснює контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;
- забезпечує організацію розмежування доступу до ресурсів ІКС Надавача;
- забезпечує спостереження за функціонуванням ІКС Надавача (реєстрація подій в ІКС Надавача, моніторинг подій тощо);
- забезпечує організацію та проведення заходів з модернізації, тестування, оперативного відновлення функціонування ІКС Надавача після збоїв, відмов, аварій;
- ведення журналу обліку адміністратора безпеки, визначеного документацією щодо КСЗІ;
- проводить перевірки відповідності положень внутрішньої організаційно-розпорядчої документації Надавача та документації щодо КСЗІ;
- здійснює контроль за дотриманням працівниками Надавача положень внутрішньої організаційно-розпорядчої документації Надавача та документації щодо КСЗІ;
- здійснює контроль за веденням баз даних Надавача;
- надає пропозиції керівництву щодо покращення умов праці.

3.1.4. Аудитор системи

- проводить перевірки цілісності архівів, журналу аудиту подій, що реєструють технічні засоби ІКС Надавача;
- забезпечує спостереження за функціонуванням КСЗІ (моніторинг та реєстрація подій в ІКС Надавача тощо);
- організовує забезпечення режиму доступу до приміщень Надавача, в яких розміщена ІКС Надавача.

3.1.5. Системний адміністратор

Функції та завдання системного адміністратора:

- відповідає за функціонування засобів та обладнання ПТК ІКС КНЕДП;
- організовує експлуатацію та технічне обслуговування ІКС КНЕДП і адміністрування її технічних засобів;

- забезпечує функціонування офіційного веб-сайту (електронного інформаційного ресурсу) КНЕДП;
- бере участь у впровадженні та забезпеченні функціонування КСЗІ;
- веде журнали аудиту подій, що реєструють технічні засоби ІКС КНЕДП;
- встановлює, налаштовує та забезпечує підтримку працездатності загальносистемного та спеціального програмного забезпечення ІКС КНЕДП, у тому числі формує та веде резервні копії його конфігурацій (конфігураційних файлів);
- встановлює та налагоджує штатну підсистему резервного копіювання бази даних ІКС КНЕДП;
- здійснює контроль за архівацією та резервуванням бази даних сформованих сертифікатів та СВС;
- забезпечує актуалізацію баз даних, які створюються та обробляються в ІКС КНЕДП, у зв'язку із збоями;
- адмініструє антивірусне програмне забезпечення, забезпечує актуальність антивірусних баз;
- здійснює технічну підтримку Підписувачів (Створювачів електронної печатки) каналами зв'язку;
- веде формуляр ІКС КНЕДП, а також відповідає за збереження апаратури та майна ІКС КНЕДП;
- отримує під час приймання чергування від чергового адміністратора реєстрації вичерпні відомості про стан процесу обробки інформації, апаратних та програмних засобів ІКС;
- звітує адміністратору безпеки та аудиту про стан процесу обробки інформації, апаратних та програмних засобів ІКС;
- готує пропозиції щодо забезпечення ПТК ІКС КНЕДП необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою з метою підвищення рівня захисту інформації;
- бере участь в інвентаризації апаратури та майна КНЕДП;
- доводить до відома розробників пропозиції та зауваження у роботі апаратних, програмних та апаратно-програмних засобів.

3.1.6. Адміністратор реєстрації

Функції та завдання адміністраторів реєстрації:

- забезпечують ідентифікацію та автентифікацію заявників, які звернулися до КНЕДП із метою формування, блокування, поновлення та скасування сертифіката;
- перевіряють документи, надані Заявниками для ідентифікації їх особи;
- перевіряють повноту комплексу документів відповідно переліку, визначеного Регламентом КНЕДП, відповідність їх оформлення вимогам Регламенту КНЕДП, а також коректність засвідчення копій документів, якими Заявник (Підписувач, Створювач електронної печатки) підтверджує дані для внесення в сертифікат;

- встановлюють належність відкритого ключа та відповідного йому особистого ключа заявнику;
- перевіряють повноту та правильність наданої Заявниками інформації, за потреби вимагають від Заявників додаткову інформацію в документальній формі, якщо така інформація необхідна для їх реєстрації;
- ведуть облік користувачів (заповнюють електронні форми з даними Підписувача (Створювача електронної печатки), перевіряють точність занесення даних, формують особову справу Підписувача (Створювача електронної печатки);
- перевіряють дані, обов'язкові для формування сертифіката, а також дані, які вносяться у сертифікат на вимогу Підписувача (Створювача електронної печатки);
- перевіряють заяви про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів Підписувача (Створювача електронної печатки), заповнюють на підставі них електронні форми про формування, скасування, блокування та поновлення сертифікатів відкритих ключів;
- надають допомогу Підписувачам (Створювачам електронної печатки) під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення, а також вживають заходів щодо забезпечення безпеки інформації під час генерації ключової інформації;
- перевіряють законність звернень про блокування, поновлення та скасування сертифікатів за процедурою, визначеною Регламентом КНЕДП;
- забезпечують документальне підтвердження заяв на зміну статусу сертифіката Підписувача (Створювача електронної печатки), які були ним сформовані та засвідчені особистим електронним підписом;
- ініціюють запити на формування стартових та робочих сертифікатів відкритих ключів Підписувачів (Створювачів електронної печатки), засвідчують коректність включених у них даних шляхом накладення на запит власного кваліфікованого електронного підпису;
- відповідають за правильність даних, включених у запит на формування сертифіката, який підписаний його електронним підписом, даним, що подані Заявником у письмовій заяві та визначених Регламентом КНЕДП документах;
- надають сертифікати відкритих ключів Підписувачам (Створювачам електронної печатки) за допомогою програмно-технічних засобів;
- засвідчують електронні заяви на блокування, поновлення та скасування сертифікатів ключів у випадках, передбачених Регламентом КНЕДП;
- надають Підписувачам (Створювачам електронної печатки) консультації щодо умов та порядку надання електронних довірчих послуг;
- забезпечують зберігання власного носія з особистим ключем, запобігання доступу до нього інших осіб;
- вносять зміни у реєстр користувачів з дозволу керівника КНЕДП або особи, що його заміщує;

- передають особові справи Підписувачів (Створювачів електронної печатки) до архіву;
- перевіряють роботу операторів реєстрації та адміністраторів реєстрації ВПР;
- відмовляють Заявнику в реєстрації та формуванні, скасуванні, блокуванні та відновленні сертифікатів ключів, якщо форма та зміст відповідної заяви не відповідають наданим документам, вимогам Регламенту КНЕДП або якщо ці заяви подає не уповноважена на це особа;
- відмовляють Підписувачу (Створювачу електронної печатки) в прийомі заяви на блокування, поновлення та скасування сертифіката за телефоном, якщо деякі з названих даних не співпадають з тими, що містяться в реєстрі користувачів.

3.1.7. Оператор реєстрації

Функції та завдання операторів реєстрації:

- забезпечують ідентифікацію осіб, які звернулися до КНЕДП із метою формування сертифіката;
- перевіряють документи, надані Заявниками для ідентифікації їх особи;
- перевіряють повноту комплексу документів відповідно переліку, визначеного Регламентом КНЕДП, відповідність їх оформлення вимогам Регламенту КНЕДП, а також коректність засвідчення копій документів, якими Заявник (Підписувач, Створювач електронної печатки) підтверджує дані для внесення в сертифікат;
- перевіряють повноту та правильність наданої Заявниками інформації, за потреби вимагають від Заявників додаткову інформацію в документальній формі, якщо така інформація необхідна для їх реєстрації;
- ведуть облік користувачів (заповнюють електронні форми з даними Підписувачів (Створювачів електронної печатки), перевіряють точність занесення даних, формують особову справу Підписувача (Створювача електронної печатки);
- перевіряють дані, обов'язкові для формування сертифіката, а також дані, які вносяться у сертифікат на вимогу Підписувача (Створювача електронної печатки);
- перевіряють заяви про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів Підписувача (Створювача електронної печатки), заповнюють на підставі них електронні форми про формування, скасування, блокування та поновлення сертифікатів відкритих ключів;
- надають допомогу Підписувачам (Створювачам електронної печатки) під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення, а також вживають заходів щодо забезпечення безпеки інформації під час генерації ключової інформації;

- отримують від Підписувачів (Створювачів електронної печатки) письмові заяви на формування, скасування, блокування та поновлення сертифікатів ключів;
- перевіряють законність звернень про блокування, поновлення та скасування сертифікатів за процедурою, визначеною Регламентом КНЕДП;
- забезпечують документальне підтвердження заяв на зміну статусу сертифіката Підписувача (Створювача електронної печатки), які були ним сформовані та засвідчені особистим електронним підписом;
- ініціюють запити на формування стартових та робочих сертифікатів відкритих ключів Підписувачів (Створювачів електронної печатки), засвідчують коректність включених у них даних шляхом накладення на запит власного кваліфікованого електронного підпису;
- відповідають за правильність даних, включених у запит на формування сертифіката, який підписаний його електронним підписом, даним, що подані Заявником у письмовій заяві та визначених Регламентом КНЕДП документах;
- засвідчують електронні заяви на блокування, поновлення та скасування сертифікатів ключів у випадках, передбачених Регламентом КНЕДП;
- надають Підписувачам (Створювачам електронної печатки) консультації щодо умов та порядку надання електронних довірчих послуг;
- забезпечують зберігання власного носія з особистим ключем, запобігання доступу до нього інших осіб;
- реєструють внесення змін у реєстр користувачів з дозволу керівника КНЕДП або особи, що його заміщує;
- передають особові справи Підписувачів (Створювачів електронної печатки) до архіву;
- перевіряють роботу операторів реєстрації та адміністраторів реєстрації ВПР;
- відмовляють Заявнику в реєстрації та формуванні, скасуванні, блокуванні та поновленні сертифікатів ключів, якщо форма та зміст відповідної заяви не відповідають наданим документам, вимогам Регламенту КНЕДП або якщо ці заяви подає не уповноважена на це особа;
- відмовляють Підписувачу (Створювачу електронної печатки) в прийомі заяви на блокування, поновлення та скасування сертифіката за телефоном, якщо деякі з названих даних не співпадають з тими, що містяться в реєстрі користувачів.

3.1.8. Чергові адміністратори реєстрації КНЕДП

Функції та завдання чергових адміністраторів реєстрації:

- забезпечують чергування у встановленому порядку;
- забезпечують безперебійне приймання звернень Підписувачів (Створювачів електронної печатки), автентифікацію Підписувача (Створювача електронної печатки), що звертається за блокуванням,

поновленням та скасуванням сертифіката (за процедурою, визначеною Регламентом КНЕДП);

- заповнюють електронні форми заяв на блокування, поновлення та скасуванням сертифікатів ключів на підставі усних заяв Підписувачів (Створювачів електронної печатки), отриманих по телефону;
- перевіряють законність звернень про блокування, поновлення та скасування за процедурою, визначеною Регламентом КНЕДП;
- відмовляють Підписувачу (Створювачу електронної печатки) в прийомі заяви про блокування, поновлення та скасуванням сертифіката телефоном, якщо деякі з названих даних не співпадають з тими, що є в реєстрі користувачів;
- забезпечують коректне та своєчасне опрацювання запиту на блокування, поновлення та скасуванням сертифіката Підписувача (Створювача електронної печатки), який звернувся з цією вимогою до КНЕДП;
- надають Підписувачам (Створювачам електронної печатки) консультації щодо умов та порядку надання електронних довірчих послуг, а також технічну підтримку Підписувачам (Створювачам електронної печатки) каналами зв'язку;
- забезпечують зберігання власного носія з особистим ключем, запобігання доступу до нього інших осіб;
- доводять до відома керівника КНЕДП або особи що, його заміщує, про всі факти блокуванням сертифікатів, що сталися протягом його чергування або за вихідні дні (з часу останньої денної зміни);

Також можуть суміщати виконання таких функцій та завдань чергових системних адміністраторів:

- ведуть постійний моніторинг функціонування ІКС КНЕДП;
- відновлюють ІКС КНЕДП після збоїв та відмов;
- підтримують під час чергування електронний інформаційний ресурс КНЕДП;
- забезпечують безперебійне функціонування ІКС КНЕДП та доступність для користувачів інформаційного ресурсу КНЕДП, а також відповідають за збереження апаратури та майна КНЕДП під час їх чергування;
- ведуть журнали, що стосуються експлуатації ІКС КНЕДП;
- звітують адміністратору безпеки та аудиту про стан процесу обробки інформації, апаратних та програмних засобів ІКС;
- доводять до відома системного адміністратора КНЕДП пропозиції та зауваження щодо роботи апаратних, програмних та апаратно-програмних засобів;
- готують пропозиції щодо забезпечення ПТК ІКС КНЕДП необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою;
- отримують під час приймання чергування від системного адміністратора КНЕДП чи іншого чергового адміністратора реєстрації КНЕДП вичерпні

відомості про стан процесу обробки інформації, апаратних та програмних засобів ІКС.

3.1.9. Посадові особи КНЕДП (керівник, заступник керівника – адміністратор сертифікації, адміністратор сертифікації, адміністратор безпеки, аудитор системи, адміністратори реєстрації, системний адміністратор, оператор реєстрації, чергові адміністратори реєстрації)

- зберігають конфіденційні відомості КНЕДП та Офісу Генерального прокурора;
- негайно доповідають про факти спроб несанкціонованого доступу до інформації, що обробляється в ІКС КНЕДП;
- дотримуються правил безпеки під час експлуатації персональних електронно-обчислювальних машин (ПЕОМ) та електрообладнання.

3.2. Відокремлені пункти реєстрації

Відокремлені пункти реєстрації створюються при необхідності провадження сервісу КНЕДП у територіально відокремлених обласних підрозділах.

Відокремлені пункти реєстрації є відокремленими регіональними підрозділами при органах прокуратури обласного рівня (обласні прокуратури), що реалізують функції КНЕДП із реєстрації заявників та їх подальшого обслуговування на відповідній території.

Відокремлені пункти діють на підставі цього Регламенту.

До складу ВПР входять:

- адміністратори реєстрації ВПР (віддалені адміністратори реєстрації);
- оператори реєстрації;
- відповідальний за захист інформації на ВПР.

Керівництво ВПР здійснює віддалений адміністратор реєстрації ВПР.

ВПР підпорядковується керівнику КНЕДП.

Функції та завдання ВПР:

- встановлення осіб, які звернулися до КНЕДП з метою формування сертифіката;
- перевірка даних, обов'язкових для формування сертифіката, а також даних, які вносяться у сертифікат на вимогу Підписувача (Створювача електронної печатки);
- проведення реєстрації Підписувачів (Створювачів електронної печатки);
- отримання від Підписувачів (Створювачів електронної печатки) заяв на формування, скасування, блокування та поновлення сертифікатів ключів;
- надання допомоги Підписувачам (Створювачам електронної печатки) під час генерації особистих та відкритих ключів у разі отримання від них

відповідного звернення та вживання заходів щодо забезпечення безпеки інформації під час генерації;

- перевірка законності звернень про блокування, поновлення та скасування сертифікатів;
- надання Підписувачам (Створювачам електронної печатки) консультацій щодо умов та порядку надання КЕДП.

Віддалені адміністратори реєстрації та оператори реєстрації відповідають за виконання функцій та несуть обов'язки адміністратора реєстрації, визначені у цьому Регламенті.

Зі складу працівників ВПР на відокремленому пункті реєстрації призначаються відповідальні за захист інформації на ВПР.

У межах виконання своїх обов'язків відповідальний за захист інформації на ВПР відповідає за належну експлуатацію комплексу засобів захисту ВПР.

Основними обов'язками відповідального за захист інформації на ВПР є:

- організація експлуатації та технічного обслуговування апаратних та програмних засобів ВПР;
- участь у впровадженні та забезпеченні функціонування комплексної системи захисту інформації у межах ВПР;
- контроль за роботою програмного комплексу ВПР;
- контроль за дотриманням політик безпеки персоналом ВПР.

4. Політика сертифіката та положення сертифікаційних практик

4.1. Перелік сфер, в яких дозволяється використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем

Сертифікати відкритого ключа, що формуються КНЕДП, використовуються для перевірки та підтвердження КЕП, який задовольняє вимогам щодо підпису, застосованого до даних в електронній формі, у той же спосіб, як власноручні підписи задовольняють вимогам стосовно документа на папері.

КНЕДП здійснює безоплатне обслуговування сертифікатів ключів, сформованих для органів прокуратури чи інших органів державної влади, їх посадових осіб та працівників для доступу до ІКС, власником/розпорядником яких є Офіс Генерального прокурора, у тому числі інформаційної системи «Система електронного документообігу органів прокуратури України».

Крім того, дозволяється використання Підписувачами, Створювачами електронної печатки вказаних сертифікатів ключів для доступу до інформаційних систем інших державних органів з метою виконання службових обов'язків, забезпечення виконання вимог антикорупційного законодавства, законодавства у сфері державної служби тощо.

Виданий КНЕДП сертифікат використовується для засвідчення чинності і належності відкритого ключа Створювачу електронної печатки, Підписувачу, автентифікації в електронних системах та системах електронного документообігу, для електронної взаємодії фізичних та юридичних осіб, яка потребує відправлення, отримання, використання та постійного зберігання за участю третіх осіб електронних даних, аналоги яких на паперових носіях повинні містити власноручний підпис чи печатку відповідно до законодавства.

КЕП, створений з використанням особистих ключів Підписувача (створювача електронної печатки) і відповідних їм сертифікатів, що формуються КНЕДП, за правовим статусом прирівнюються до власноручного підпису та печатки і можуть використовуватися в усіх сферах, де використовується власноручний підпис посадових осіб чи печатка.

4.2. Обмеження щодо використання кваліфікованих сертифікатів відкритих ключів, сформованих надавачем

КНЕДП має право встановлювати обмеження сфери використання сформованих ним сертифікатів ключів. Інформація щодо обмеження сфери використання застосовується відповідно до вимог законодавства, доводиться до Підписувача (Створювача електронної печатки, Заявника) та зазначається у сформованому КНЕДП сертифікаті ключа.

4.3. Перелік інформації, що розміщується надавачем на своєму офіційному веб-сайті (інформаційному ресурсі КНЕДП)

Інформаційний ресурс КНЕДП (офіційний веб-сайт) призначений для розміщення на ньому відкритої інформації, яка структурно поділяється на:

- відомості про Надавача (загальні відомості про КНЕДП та його ВПР, розпорядок їх роботи та контактні дані);
- дані про внесення відомостей про КНЕДП до Довірчого списку;
- кваліфіковані сертифікати відкритих ключів Надавача (КНЕДП, серверів КНЕДП)
- перелік кваліфікованих електронних довірчих послуг, які надає 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 (СВС та дельта-СВС, які містять інформацію про статуси сертифікатів КНЕДП та Підписувачів, що відкликані);
- відомості про обмеження під час використання кваліфікованих сертифікатів відкритих ключів користувачами;
- 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;
- положення цього Регламенту (визначені для розповсюдження);
- прикладне програмне забезпечення.

Електронна адреса (DNS-ім'я) електронного інформаційного ресурсу: <https://ca.gp.gov.ua>.

Технічною основою інформаційного ресурсу КНЕДП є веб-сервер, що входить до складу ПТК КНЕДП.

Сертифікат КНЕДП, сертифікати функціональних серверів КНЕДП (OCSP, TSP), СВС та сертифікати розміщуються:

- у складі веб-сторінок на веб-сервері КНЕДП;
- в інформаційному дереві LDAP-каталогу на LDAP-сервері.

Сертифікати Підписувачів (Створювачів електронної печатки) розміщуються в LDAP-каталозі та доступні прикладному ПЗ після авторизації.

Доступ до веб-сервера здійснюється за DNS-ім'ям <https://ca.gp.gov.ua> за протоколом HTTP(S) (номер TCP-порту 80, 443).

4.4. Час і порядок публікації кваліфікованих сертифікатів відкритих ключів та списків відкликаних сертифікатів

На інформаційному ресурсі КНЕДП виконується публікація сертифікатів:

- КНЕДП;
- сервера позначок часу (TSP-сервера);
- сервера визначення статусу сертифікатів (OCSP-сервера);
- сервера управління сертифікатами (CMP-сервера).

Після отримання сертифікатів відкритих ключів КНЕДП та серверів позначок часу КНЕДП, формування сертифікатів відкритих ключів серверів визначення статусу сертифікатів та управління сертифікатами вони автоматично публікуються ПТК в LDAP-каталозі. Інформаційний ресурс отримує сертифікати з LDAP при кожному зверненні з відповідної веб-сторінки.

Сертифікати Підписувачів (Створювачів електронної печатки), враховуючи їх відомчу належність, на інформаційному ресурсі КНЕДП не публікуються. Вони доступні для Підписувачів (Створювачів електронної печатки) через прикладне ПЗ відомчої інформаційної системи, яка отримує їх після автентифікації з LDAP-каталогу.

Для розповсюдження інформації про статус сертифікатів ключів Підписувачів (Створювачів електронної печатки) використовується механізм списку відкликаних сертифікатів та механізм визначення статусу сертифіката ключа в режимі реального часу за протоколом OCSP.

КНЕДП надає всім користувачам послугу інтерактивного визначення статусу сертифіката. Послуга надається шляхом відправлення запиту за протоколом HTTP на OCSP-сервер КНЕДП.

Публікація СВС Підписувачів (Створювачів електронної печатки) у LDAP-каталозі здійснюється одразу після його випуску.

Інформаційний ресурс Надавача отримує СВС із LDAP при кожному зверненні до відповідної веб-сторінки.

СВС випускається кожні дві години та містить інформацію про всі відкликані (скасовані, заблоковані, поновлені) сертифікати.

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

Повний список відкликаних сертифікатів формується та публікується 1 (один) раз на добу та містить інформацію про всі відкликані (скасовані, заблоковані, поновлені) сертифікати ключів, які були сформовані Надавачем.

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

сертифікатів та часом формування поточного часткового списку відкликаних сертифікатів.

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

Генерація пари ключів заявника здійснюється за його особистої присутності у приміщенні КНЕДП або приміщенні його ВПР після ідентифікації такого Підписувача (Створювача електронної печатки), перевірки достатності обсягу його цивільної правоздатності і дієздатності, формування та видачі йому кваліфікованого сертифіката відкритого ключа на підставі засвідчення відповідальним працівником надавача факту володіння Підписувачем (Створювачем електронної печатки) особистим ключем, що відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката відкритого ключа.

Підтвердження володіння Підписувачем (Створювачем електронної печатки) особистим ключем здійснюється без розкриття особистого ключа.

4.6. Умови встановлення заявника

4.6.1. Загальні положення

Для отримання КЕДП особа, яка звернулася до Надавача, повинна бути встановлена (ідентифікована, автентифікована) відповідно до вимог законодавства у сфері надання КЕДП та електронної ідентифікації і Регламенту.

Ідентифікація, автентифікація Заявників, Підписувачів та створювачів електронної печатки здійснюється Надавачем у випадках:

- звернення до Надавача із заявою про реєстрацію;
- звернення до Надавача із заявою на зміну статусу сертифіката (скасування, блокування, поновлення сертифіката), повторне формування сертифіката;
- встановлення Надавачем належності відкритого ключа та відповідного йому особистого ключа Заявнику.

Ідентифікація особи здійснюється кваліфікованим надавачем електронних довірчих послуг (його відокремленим пунктом реєстрації) шляхом перевірки та підтвердження належності юридичній особі, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, ідентифікаційних даних особи, отриманих кваліфікованим надавачем електронних довірчих послуг (його відокремленим пунктом реєстрації).

Відповідно до статті 22 Закону формування та видача надавачем, його відокремленим пунктом реєстрації, кваліфікованого сертифіката відкритого ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті відкритого ключа, не допускаються.

Кваліфікований надавач електронних довірчих послуг під час формування та видачі кваліфікованого сертифіката відкритого ключа працівнику юридичної особи здійснює ідентифікацію працівника, а також ідентифікацію особи уповноваженого представника юридичної особи відповідно до вимог статті 22 та перевіряє обсяг його повноважень за документом, що визначає повноваження уповноваженого представника юридичної особи, чи з використанням інформації, що міститься в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань або в торговельному, банківському чи судовому реєстрі.

Проводити під час видачі засобів електронної ідентифікації перевірку інформації про осіб, яким видаються такі засоби, з використанням відомостей інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ України (відомостей, що містяться в Єдиному державному демографічному реєстрі, та відомостей щодо викрадених (втрачених) документів - за зверненнями), Державного реєстру фізичних осіб - платників податків, Державного реєстру актів цивільного стану громадян, Єдиного державного реєстру юридичних осіб, фізичних осіб - підприємців та громадських формувань, а також інформації з інших публічних електронних реєстрів відповідно до Закону України «Про публічні електронні реєстри», отриманих у процесі електронної взаємодії за допомогою інтегрованої системи електронної ідентифікації в порядку, визначеному Кабінетом Міністрів України.

Усі процедури з обслуговування Підписувачів (Створювачів електронної печатки) здійснюються після їх ознайомлення з такими положеннями цього Регламенту:

- права та обов'язки Підписувача (Створювача електронної печатки) і КНЕДП, ВГП та їх відповідальність;
- порядок ідентифікації та реєстрації Підписувача (Створювача електронної печатки);
- порядок генерації ключів КЕП;
- порядок формування сертифікатів;
- сфери використання кваліфікованого сертифіката та обмеження щодо його використання;
- порядок перевірки чинності кваліфікованого сертифіката;
- порядок блокування, скасування та поновлення сертифіката, який викладено в цьому розділі.

Встановлення особи Заявника, Підписувача та Створювача електронної печатки здійснюється за механізмами, визначеними цим Регламентом, які передбачають:

- перевірку ідентифікаційних даних за документами або іншими відомостями, у тому числі в електронній формі, що підтверджують ідентифікаційні дані;
- голосову автентифікацію за ключовою фразою.

Ідентифікація за документами або іншими відомостями, у тому числі в електронній формі, що підтверджують ідентифікаційні дані осіб, які звернулись до Надавача, здійснюється адміністратором реєстрації Надавача чи віддаленим адміністратором реєстрації. Ідентифікація фізичної особи – представника юридичної особи чи державної установи, яка звернулася за отриманням КЕД послуг, здійснюється за умови її особистої присутності.

Голосова автентифікація за ключовою фразою здійснюється адміністратором реєстрації Надавача чи віддаленим адміністратором реєстрації у випадках подання заяви про блокування, поновлення та скасування кваліфікованого сертифіката в усній формі.

4.6.2. Порядок ідентифікації та реєстрації Підписувачів (Створювачів електронної печатки, Заявників)

Під реєстрацією Підписувача (Створювача електронної печатки) розуміється внесення інформації про Підписувача (Створювача електронної печатки) до реєстру Підписувачів (Створювачів електронної печатки) КНЕДП.

Проведення реєстрації здійснюється в КНЕДП (ВІР) у робочий час згідно з розпорядком роботи КНЕДП (ВІР).

Для проведення реєстрації особа подає до КНЕДП заяву про проведення реєстрації та комплект документів за переліком та у порядку, що визначені у цьому Регламенті та порядку, затверджені постановою Кабінету Міністрів України від 01.08.2023 № 798.

Для проведення реєстрації особа (Заявник), яка бажає стати Підписувачем, повинна надати до КНЕДП (ВІР) такі документи:

- заяву на проведення реєстрації та формування кваліфікованого сертифіката відкритого ключа електронного підпису (додаток № 1 до Регламенту);
- оригінал паспорта або паспорта заявника, виготовленого у формі ID-картки, що містить безконтактний електронний носій (також надаються засвідчені підписом власника копії 1–2 сторінок паспорта (3–6 за наявності відміток) або лицьового та зворотного боку ID-картки);
- оригінал картки фізичної особи – платника податків з реєстраційним номером облікової картки платника податків (далі – РНОКПП) та її копію, засвідчену підписом власника (у разі якщо через релігійні переконання посадова особа відмовилася від РНОКПП не подається, однак надається засвідчена підписом власника копія відповідної сторінки паспорта з відміткою про це);
- копію наказу або витяг з наказу, або довідку кадрового підрозділу про призначення на посаду (перебування на посаді), що завірена належним

чином. Вказаний документ має бути видано/посвідчено не пізніше 5 днів до звернення до КНЕДП (ВІР).

Документи (заява, копії паспортів тощо) засвідчуються підписом Заявника (Підписувача) та звіряються уповноваженою особою КНЕДП, якій надаються копії разом з оригіналами. Використання факсимільного підпису під час засвідчення документів не допускається.

Заявник зобов'язаний надати свої контактні дані, в тому числі номер телефону та адресу електронної пошти, за допомогою якої можна зв'язатися з ним.

Для проведення реєстрації уповноважена посадова особа (Заявник) органу прокуратури чи іншого державного органу, який бажає стати Створювачем електронної печатки, повинен надати до КНЕДП (ВІР) такі документи:

- заяву на проведення реєстрації та формування кваліфікованого сертифіката відкритого ключа електронної печатки (додаток № 2 до Регламенту);
- копію організаційно-розпорядчого документа про створення чи початок роботи відповідного органу прокуратури чи іншого державного органу або копію витягу з Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань. Вказаний документ має бути посвідчено не пізніше 5 днів до звернення до КНЕДП (ВІР);
- копію наказу (копії наказів) керівництва органу прокуратури чи іншого державного органу про використання відповідної печатки та осіб, які відповідальні за її отримання і правильне застосування. Вказаний документ має бути посвідчено не пізніше 5 днів до звернення до КНЕДП (ВІР);
- оригінал паспорта або паспорта уповноваженої особи, виготовленого у формі ID-картки, що містить безконтактний електронний носій (також надаються засвідчені власноручним підписом власника копії 1–2 сторінок паспорта (3–6 за наявності відміток) або лицьового та зворотного боку ID-картки);
- копію наказу або витяг з наказу, або довідку кадрового підрозділу про призначення на посаду (перебування на посаді), що завірена належним чином. Вказаний документ має бути видано/посвідчено не пізніше 5 днів до звернення до КНЕДП (ВІР).

Документи (заява, копії паспортів тощо) засвідчуються власноручним підписом уповноваженої посадової особи Заявника (Створювача електронної печатки) з накладенням на заяву відтиску відповідної печатки та звіряються уповноваженою особою КНЕДП, якій надаються копії разом з оригіналами. Використання факсимільного підпису під час засвідчення документів не допускається.

До розгляду не приймаються документи, які мають підчистки, дописки, закреслені слова, інші незастережні виправлення або написи олівцем, а також пошкодження, внаслідок чого їх текст неможливо прочитати.

Бланки реєстраційних документів (заява на проведення реєстрації та формування кваліфікованого сертифіката тощо) встановленої форми розміщуються на інформаційному ресурсі КНЕДП.

4.6.3. Процедура проведення реєстрації Заявника

Особа, що звертається до КНЕДП для формування сертифіката, подає документи оператору реєстрації КНЕДП (ВІР).

Оператор реєстрації виконує процедуру ідентифікації особи, яка проходить процедуру реєстрації, шляхом установлення особи за паспортом громадянина України.

При ідентифікації посадової особи з'ясовують:

- прізвище, ім'я та по батькові;
- дату народження;
- серію і номер паспорта громадянина України, дату видачі та орган, що його видав;
- реєстраційний номер облікової картки платника податків (РНОКПП) або відмітку в паспорті.

Після позитивної ідентифікації оператор реєстрації приймає та розглядає документи, надані особою.

Оператор реєстрації КНЕДП (ВІР) приймає рішення про відмову в реєстрації за результатом розгляду поданих документів у разі:

- відсутності необхідних для реєстрації документів;
- подання заявником неналежно засвідчених копій документів чи документів, які мають підчистки, дописки, закреслені слова, інші незастережні виправлення або написи олівцем, а також пошкодження, внаслідок чого їх текст неможливо прочитати;
- невідповідності даних, що визначені в поданих документах, фактичним даним Підписувача (Створювача електронної печатки, Заявника);
- відсутності у посадової особи іншого державного органу повноважень для доступу до ІКС, власником/розпорядником яких є Офіс Генерального прокурора.

У разі відмови в реєстрації заява на реєстрацію разом з додатками повертається заявнику з позначкою оператора реєстрації КНЕДП (ВІР).

При ухваленні позитивного рішення оператор реєстрації КНЕДП (ВІР) виконує реєстраційні дії щодо занесення реєстраційної інформації до електронного реєстру Підписувачів (Створювачів електронної печатки) КНЕДП, формує справу Підписувача (Створювача електронної печатки) та долучає до неї необхідні оригінали чи належним чином засвідчені копії документів.

Справи Підписувачів (Створювачів електронної печатки) зберігаються в металевих шафах, що забезпечують надійний захист від несанкціонованого доступу, в КНЕДП (ВІР).

Оператор реєстрації проводить інформування Підписувача (Створювача електронної печатки) щодо порядку надання КЕДП, визначених цим Регламентом правил поводження з особистими ключами, особливостей і обмежень використання сертифіката.

Реєстрація заявника є підставою для процесу генерації пари ключів (особистого та відкритого), що здійснюється підписувачем - представником державної установи із використанням засобів КЕП за його особистої присутності у КНЕДП (ВІПР) та формування сертифіката ключа Підписувача (Створювача електронної печатки).

Адміністратор реєстрації, як і оператор реєстрації, може проводити процедури з ідентифікації та реєстрації Заявника (Підписувача, Створювача електронної печатки).

4.7. Механізм автентифікації користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований надавачем

Підписувач (Створювач електронної печатки) може бути автентифікований Надавачем за ідентифікаційними даними, що містяться у раніше сформованому Надавачем кваліфікованому сертифікаті цього Підписувача (Створювача електронної печатки), за умов чинності такого сертифіката та незмінності його ідентифікаційних даних на момент звернення для отримання КЕД послуги.

Підписувач (Створювач електронної печатки) зобов'язаний у разі зміни своїх ідентифікаційних даних, що містяться у кваліфікованому сертифікаті, сформованому Надавачем, до отримання КЕД послуги з проведенням його автентифікації за даними такого сертифіката, звернутися до Надавача з повідомленням про настання відповідних змін та надати документи, що їх підтверджують, для скасування чинного кваліфікованого сертифіката та формування нового з новими ідентифікаційними даними.

4.8. Механізм встановлення користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа

Ідентифікація та автентифікація Заявників, Підписувачів, Створювачів електронної печатки під час подання заяв щодо скасування, блокування та поновлення сертифікатів здійснюється у порядку, встановленому розділом 4.20 цього Регламенту.

4.9.

4.13.5. Процес, порядок та умови генерації пар ключів користувачів

Генерація пари ключів (особистого та відкритого) здійснюється особисто заявниками із використанням засобів кваліфікованого електронного підпису за їх особистої присутності у приміщенні надавача чи його відокремленого пункту реєстрації під контролем адміністратора реєстрації або оператора реєстрації.

Існує можливість генерації ключової пари підписувачем у Хмарному сховищі Надавача, яке реалізує зберігання особистих ключів користувача, що може функціонувати під управлінням або з використанням окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків та які перебувають у власності користувачів або надаються Надавачем, така генерація ініціюється підписувачем самостійно після авторизації у Хмарному сховищі на основі атрибутів захисту від доступу сторонніх осіб до використання особистого ключа (пароль, PIN-код, використання двофакторної автентифікації тощо).

Особистий ключ Підписувача (Створювача електронної печатки) генерується засобом КЕП (зокрема ЗНОК) та захищається паролем. Відповідальність за забезпечення конфіденційності, цілісності та неможливості доступу інших осіб до особистого ключа, а також неможливість ознайомлення із значенням параметрів особистого ключа (паролем) та його копіювання несе сам Підписувач, уповноважений представник Створювача електронної печатки.

Засоби КЕП під час генерації ключів формують запит на формування сертифіката (запит на сертифікацію) формату PKCS#10, що містить відкритий ключ Підписувача (Створювача електронної печатки) і додаткову інформацію для формування кваліфікованого сертифіката у Надавача.

Особистий ключ Підписувача (Створювача електронної печатки), що відповідає відкритому ключу, кваліфікований сертифікат відкритого ключа який сформовано надавачем, використовується відповідно до переліку сфер використання сертифіката, основних обмежень та інших даних, включених до кваліфікованого сертифіката відкритого ключа Підписувача (Створювача електронної печатки) на його вимогу.

Паролі захисту особистих ключів користувачів у Надавача не зберігаються.

4.16.

4.17. Процедури отримання користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги її надавачем

Особистий ключ Підписувача (Створювача електронної печатки) генерується особисто Підписувачем, уповноваженим представником Створювача електронної печатки на засобі КЕП або у Хмарному сховищі та залишається у Підписувача, уповноваженого представника Створювача електронної печатки.

Особисті ключі Підписувачів (Створювачів електронної печатки) не передаються КНЕДП та не зберігаються у Надавача чи його ВІПР.

4.18. Механізм надання відкритого ключа користувача надавачу для формування кваліфікованого сертифіката відкритого ключа

Відкритий ключ Підписувача (Створювача електронної печатки) формується під час генерації ключів засобами КЕП та подається Надавачу у запиті на сертифікацію, що є файлом формату PKCS#10.

Умови подання запиту на сертифікацію встановлено пунктом 4.19.1 цього Регламенту.

4.19. Положення сертифікаційних практик

4.19.1. Процес подання запиту на формування кваліфікованого сертифіката відкритого ключа Підписувача (Створювача електронної печатки)

Формування кваліфікованого сертифіката відкритого ключа Підписувачу чи Створювачу електронної печатки здійснюється на підставі заяви про формування кваліфікованого сертифікату відкритого ключа електронного підпису чи печатки (згідно з додатком № 1 цього Регламенту), яка подається у порядку, встановленому розділом 4.6 цього Регламенту.

Для використання КЕП відповідно до асиметричних алгоритмів ДСТУ 4145-2002, ECDSA, RSA визначеного ДСТУ 4145-2002, ДСТУ ISO/IEC 14888-3:2015, PKCS#1 v2.2 (RFC 8017), відповідно, Підписувач (Створювач електронної печатки) повинен згенерувати пару ключів – відкритий та особистий.

Генерація ключів КЕП може проходити у один чи два етапи згідно з такими процедурами:

- 1) У цьому варіанті процедура генерації відбувається в два етапи:
 - генерація стартових ключів;
 - генерація робочих ключів.

За введеними під час реєстрації даними оператор реєстрації генерує стартові ключі за допомогою ПЗ. При цьому ключова пара в захищеному вигляді зберігається на ЗКЕП, що видається в користування Підписувачу (Створювачу електронної печатки) КНЕДП (ВІР) або надається самим Заявником. Так, ключовий контейнер може зберігатися у шифрованому вигляді як файл або на апаратному захищеному ЗКЕП.

Пароль доступу до ключа у шифрованому файловому контейнері або апаратному захищеному ЗКЕП вводиться оператором реєстрації та повідомляється Підписувачу (представнику Створювача електронної печатки).

Запит на формування стартового сертифіката засвідчується КЕП оператора реєстрації та відправляється електронними засобами до КНЕДП. Стартовий сертифікат відкритого ключа формується КНЕДП в автоматичному режимі, відправляється та записується ПЗ разом із ланцюжком сертифікатів КНЕДП до засобу КЕП.

Після формування стартового сертифіката оператор реєстрації чи адміністратор реєстрації на вимогу Підписувача (представника Створювача електронної печатки) виготовляє дві копії стартового сертифіката у вигляді документа у паперовій формі. Копії сертифікатів засвідчуються власноручним підписом Підписувача (представника Створювача електронної печатки), а також власноручним підписом оператора реєстрації чи адміністратора реєстрації, а Підписувач (представник Створювача електронної печатки) на другій копії сертифіката ставить відмітку про отримання такої копії.

Оператор реєстрації чи адміністратор реєстрації видає засіб КЕП Підписувачу (Створювачу електронної печатки).

Підписувач (представник Створювача електронної печатки) підключає свій ЗКЕП до відокремленого комп'ютера, що не підключений до мережі. За допомогою ПЗ генерації ключів Підписувач (представник Створювача електронної печатки) генерує робочу ключову пару. Під час генерації особистий ключ зберігається на ЗКЕП Підписувача (Створювача електронної печатки). Одночасно Підписувач (представник Створювача електронної печатки) вводить новий пароль доступу до засобу КЕП.

Запит на робочий сертифікат є самопідписаним та підписаний стартовим ключем, Підписувач (представник Створювача електронної печатки) записує на технологічний носій та передає його адміністратору реєстрації.

У разі генерації ключа у Хмарному сховищі Надавача, оператор ініціює створення віртуального токена для Підписувача програмними засобами КНЕДП, де використовує паролі для доступу, який система згенерувала під-час створення віртуального токена і в подальшому буде передано користувачу для формування запиту на сертифікат і автоматичного відправлення даного запиту Начавачу для підтвердження Адміністратором реєстрації.

Користувач самостійно генерує запит на формування стартового сертифіката, який в подальшому засвідчується КЕП оператора реєстрації та відправляється електронними засобами до КНЕДП. Стартовий сертифікат відкритого ключа формується КНЕДП в автоматичному режимі, відправляється та записується ПЗ разом із ланцюжком сертифікатів КНЕДП.

Стартовий сертифікат після проходження реєстрації в КНЕДП автоматично змінює статус на діючий і записується до віртуального токена користувача, який знаходиться у Хмарному сховищі.

Користувач Хмарного сховища, зобов'язаний самостійно змінити паролі доступу до сховища та пін-код до віртуального токена, також необхідно додати двофакторну автентифікацію.

- 2) У цьому варіанті процедура генерації відбувається в один етап:
 - генерація робочих ключів.

За введеними під час реєстрації даними оператор реєстрації генерує зразу робочі ключі за допомогою ПЗ. При цьому ключова пара в захищеному вигляді зберігається на ЗКЕП, що видається в користування Підписувачу (Створювачу електронної печатки) КНЕДП (ВІР) або надається самим Заявником. Так, ключовий контейнер може зберігатися у шифрованому вигляді як файл або на апаратному захищеному ЗКЕП.

Оператор реєстрації чи адміністратор реєстрації видає засіб КЕП Підписувачу (Створювачу електронної печатки).

Пароль доступу до ключа у шифрованому файловому контейнері або апаратному захищеному ЗКЕП вводиться Підписувачем (представником Створювача електронної печатки) у спосіб, що унеможливує його розголошення, та не повідомляється оператору реєстрації.

Підписувач (представник Створювача електронної печатки) підключає свій ЗКЕП до комп'ютера оператора чи адміністратора реєстрації, що підключений до мережі. За допомогою ПЗ оператора чи адміністратора реєстрації Підписувач (Створювач електронної печатки) генерує робочу ключову пару. Під час генерації особистий ключ зберігається на ЗКЕП Підписувача (представник Створювача електронної печатки). Одночасно

Підписувач (представник Створювача електронної печатки) вводить новий пароль доступу до засобу КЕП.

Запит на формування робочого сертифіката передається оператору реєстрації, засвідчується КЕП оператора реєстрації та відправляється електронними засобами до КНЕДП. Робочий сертифікат відкритого ключа формується КНЕДП в автоматичному чи ручному режимі, відправляється та записується ПЗ разом із ланцюжком сертифікатів КНЕДП до засобу КЕП.

Після формування запиту на робочий сертифікат оператор реєстрації чи адміністратор реєстрації на вимогу Підписувача (представника Створювача електронної печатки) виготовляє дві копії запиту на робочий сертифікат у вигляді документа у паперовій формі. Копії запиту на сертифікат засвідчуються власноручним підписом Підписувача (представника Створювача електронної печатки), а також власноручним підписом оператора реєстрації чи адміністратора реєстрації, а Підписувач (представник Створювача електронної печатки) на другій копії запиту на сертифікат ставить відмітку про отримання такої копії.

4.19.2. Порядок формування сертифікатів та надання їх користувачу

Формування сертифіката Підписувача (Створювача електронної печатки) проводиться в КНЕДП за запитом, який надходить від адміністратора реєстрації.

Формування сертифіката може бути первинним (під час першого звернення Заявника до КНЕДП) та повторним. Повторне формування сертифіката проводиться в таких випадках:

- закінчення строку чинності сертифіката ключа;
- скасування сертифіката за заявою власника;
- зміна даних, що вносяться до сертифіката ключа;
- компрометація особистого ключа.

а) Порядок первинного формування сертифіката

Процедура формування сертифіката відкритого ключа Підписувача (Створювача електронної печатки) проводиться після успішного завершення процедур реєстрації та генерації робочих ключів.

Адміністратор реєстрації перевіряє коректність даних Підписувача (Створювача електронної печатки), що внесені в запит на формування сертифіката.

Після позитивної перевірки поданого запиту з відкритим ключем адміністратор реєстрації за допомогою ПЗ засвідчує запит власним ключем КЕП та відправляє до КНЕДП для формування сертифіката.

Запит відправляється внутрішньою електронною поштою до серверу застосувань КНЕДП, який повертає електронну квитанцію про отримання запиту. При цьому статус запиту на формування сертифіката в електронному

реєстрі КНЕДП (ВПР) змінюється на «Прийнятий ЦСК». Якщо квитанція про отримання не надійшла та статус залишився «Відправлений» протягом 15 хв, адміністратор реєстрації повторює відправлення запиту до КНЕДП.

Після того, як запит на формування сертифіката засвідчується особистим ключем адміністратора сертифікації, сервер застосувань КНЕДП формує сертифікат та засвідчує його особистим ключем КНЕДП.

Після формування сертифікат публікується в LDAP-каталозі та відсилається до КНЕДП (ВПР), з якого надійшов запит, внутрішньою електронною поштою у вигляді квитанції.

Сертифікат в електронній формі записується на ЗКЕП Підписувача (Створювача електронної печатки) на робочій станції генерації ключів, якщо запис кваліфікованого сертифіката відкритого ключа Підписувача (Створювача електронної печатки) здійснюється в КНЕДП (ВПР).

Якщо запис кваліфікованого сертифіката відкритого ключа Підписувача (Створювача електронної печатки) здійснюється на робочому місці Підписувача (Створювача електронної печатки), то отримання сертифіката з LDAP-каталогу та запис його до засобу КЕП здійснює прикладне ПЗ користувача при першому використанні ключів.

б) Порядок повторного формування сертифіката

Повторне формування сертифіката не потребує проведення реєстраційних дій, крім випадку зміни даних, відображених у сертифікаті ключа.

Для ідентифікації користувача необхідно надати оригінал (для ознайомлення) паспорта громадянина України (паспорта громадянина України для виїзду за кордон, електронного відображення паспорта громадянина України / паспорта громадянина України для виїзду за кордон разом з унікальним електронним ідентифікатором (QR-кодом, штрих-кодом, цифровим кодом), та надання копії цього документа, засвідченої відповідно до чинного законодавства.

У випадку зміни даних реєстрація проводиться відповідно до п. 4.6.1 цього Регламенту, подається заява, але до неї додаються тільки документи, які містять відомості, в яких відбулися зміни.

Крім того, пред'являється засіб КЕП, якщо такий раніше видавався Підписувачеві (Створювачеві електронної печатки) у користування цим КНЕДП (ВПР).

4.19.3. Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа користувача на офіційному веб-сайті надавача

Після формування сертифіката Підписувача (Створювача електронної печатки) вони автоматично публікуються в LDAP-каталозі. Інформаційний

ресурс отримує сертифікати з LDAP при кожному зверненні з відповідної веб-сторінки.

Сертифікати Підписувачів (Створювачів електронної печатки), враховуючи їх відомчу належність, на інформаційному ресурсі КНЕДП не публікуються. Вони доступні для Підписувачів (Створювачів електронної печатки) через прикладне ПЗ відомчої інформаційної системи, яка отримує їх після автентифікації з LDAP-каталогу.

4.19.4. Умови використання кваліфікованого сертифіката відкритого ключа користувача та його особистого ключа

Кваліфікований електронний підпис чи печатка вважається таким, що пройшов перевірку та отримав підтвердження, якщо перевірку кваліфікованого електронного підпису чи печатки проведено засобом КЕП відповідно до вимог частини 2 статті 18 Закону.

Кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису.

Кваліфікована електронна печатка має презумпцію цілісності електронних даних і достовірності походження електронних даних, з якими вона пов'язана.

Результати наданих надавачем КЕДП повинні визнаватися в усіх державних установах та іншими користувачами цих послуг.

Електронний підпис чи печатка не можуть бути визнані недійсними виключно на тій підставі, що вони мають електронний вигляд або не відповідають вимогам до кваліфікованого електронного підпису чи печатки.

Шкода, заподіяна користувачеві електронних довірчих послуг надавачем підлягає відшкодуванню у повному розмірі в установленому законом порядку.

Особи, винні в порушенні вимог цього Регламенту та порядку використання електронних довірчих послуг, визначеного Законом та нормативно-правовими актами у сфері електронних довірчих послуг несуть відповідальність відповідно до статті 36 Закону.

Спори, що виникають під час надання надавачем електронних довірчих послуг та їх використання, вирішуються в порядку, встановленому законом.

Умови використання Підписувачем (Створювачем електронної печатки) особистого ключа та власного кваліфікованого сертифіката, а також використання користувачами кваліфікованих сертифікатів інших Підписувачів визначені у розділі 4.1 Регламенту.

4.20. 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)

4.20.1. Причини, за яких Підписувач (Створювач електронної печатки) зобов'язаний скасувати сертифікат

Підписувач (Створювач електронної печатки) зобов'язаний виконати дії зі скасування свого сертифіката у разі:

- компрометації особистого ключа;
- зміни відомостей, зазначених у сертифікаті.

У випадках:

- смерті Підписувача або оголошення його померлим чи безвісно відсутнім за рішенням суду;
- визнання Підписувача недієздатним, обмеження його дієздатності за рішенням суду;
- набрання законної сили рішенням суду про скасування кваліфікованого сертифіката відкритого ключа;
- звільнення з посади у відповідному органі;
- припинення діяльності відповідного органу чи його підрозділу;
- припинення використання відповідної електронної печатки

керівництво установи, до якої належить Підписувач, зобов'язане повідомити КНЕДП про ці події письмово з наданням завірених копій документів, що підтверджують цю подію. КНЕДП скасовує сертифікат відкритого ключа Підписувача (Створювача електронної печатки) при надходженні документів чи належним чином завірених копій, які посвідчують вказані вище факти.

Надавач автоматично скасовує сертифікат у разі закінчення строку його чинності або при надходженні інформації про припинення діяльності відповідного органу, у якому працював Підписувач чи була створена печатка, про факт компрометації особистого ключа Підписувача (Створювача електронної печатки) чи надання Підписувачем (Створювачем електронної печатки) недостовірних даних, якщо достовірність цієї інформації підтверджена, а також набрання законної сили рішенням суду про скасування кваліфікованого сертифіката відкритого ключа, оголошення Підписувача померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності, визнання користувача електронних довірчих послуг банкрутом.

Компрометація ключа Підписувача (Створювача електронної печатки) – це:

- факт або обґрунтована підозра того, що особистий ключ Підписувача (Створювача електронної печатки) став відомий або доступний до використання іншим особам;

- факт втрати Підписувачем (Створювачем електронної печатки) можливості подальшого використання особистого ключа з будь-яких обставин (зокрема вихід з ладу або втрата носія)

У разі компрометації ключа Підписувач (Створювач електронної печатки) зобов'язаний терміново сповістити про цей факт КНЕДП та виконати дії згідно з пунктом 4.20.3 цього Регламенту.

Сертифікат Підписувача (Створювача електронної печатки) буде скасовано у разі надання до КНЕДП третьою особою загубленого/вилученого засобу КЕП Підписувача (Створювача електронної печатки) та підтвердження його справжності (співпадіння внутрішнього ідентифікаційного номера засобу КЕП чи ідентифікатору відкритого ключа Підписувача (Створювача електронної печатки)).

Зміна будь-якої з відомостей, що зазначені в сертифікаті, потребує його скасування.

Зокрема, до таких причин належать:

- переведення на іншу посаду або звільнення з роботи власника сертифіката;
- зміна прізвища, ім'я, по батькові;
- зміна найменування юридичної особи чи її підрозділу;
- виявлення помилок у реквізитах тощо.

У разі виникнення будь-яких причин та обставин, зазначених вище, Підписувач (Створювач електронної печатки) зобов'язаний невідкладно заблокувати сертифікат згідно з пунктом 4.20.3 та протягом терміну дії блокування виконати операції зі скасування сертифіката згідно з пунктом 4.20.8 цього Регламенту.

Дозволяється виконувати безпосередньо скасування сертифіката (оминаючи фазу його блокування).

Документи, що були підставою для скасування, блокування або поновлення сертифіката ключа, фіксуються та зберігаються у КНЕДП.

4.20.2. Порядок блокування сертифікатів

Блокування тимчасово припиняє дію сертифіката. Після блокування сертифіката Підписувач (Створювач електронної печатки) зобов'язаний або поновити сертифікат згідно з пунктом 4.20.14, або виконати скасування сертифіката згідно з пунктом 4.20.8 цього Регламенту. Для здійснення блокування сертифіката Підписувач (Створювач електронної печатки) подає заяву про блокування до КНЕДП (додаток № 3 до Регламенту).

Блокування сертифіката здійснюється КНЕДП на підставі заяви, що надходить в установленому порядку до КНЕДП (ВІПР) або черговому адміністратору реєстрації в усній або паперовій формі.

Часом блокування сертифіката вважається час внесення інформації про зміну статусу сертифіката до СВС.

4.20.3. Блокування сертифіката за заявою в усній формі

Заява про блокування в усній формі подається черговому адміністратору реєстрації за телефоном.

Підписувач (Створювач електронної печатки) повинен повідомити відповідній посадовій особі КНЕДП таку інформацію:

- своє прізвище, ім'я та по батькові;
- ключову фразу-пароль.

Заява в усній формі приймається тільки при збігу даних Підписувача (Створювача електронної печатки) та фрази-пароля, переданих у заяві, з інформацією, що знаходиться в реєстрі Підписувачів (Створювачів електронної печатки).

Приймання та обробка усної заяви здійснюються у робочий час відповідною особою КНЕДП (ВПР) або цілодобово черговим адміністратором реєстрації. Обробка усної заяви про блокування сертифіката здійснюється безпосередньо після приймання заяви.

Черговий адміністратор реєстрації після перевірки повідомлених даних за допомогою ПТК формує запит на блокування сертифіката та передає його до КНЕДП.

4.20.4. Блокування сертифіката за заявою в паперовій формі

Заява в паперовій формі подається до КНЕДП (ВПР) за відповідною формою (додаток № 3 до Регламенту).

Заява про блокування сертифіката засвідчується власноручним підписом власника сертифіката.

Подання заяви в паперовій формі про блокування сертифіката та її розгляд здійснюються тільки в робочий час відповідно до розпорядку роботи КНЕДП (ВПР).

Під час приймання заяви оператор реєстрації чи адміністратор реєстрації КНЕДП проводить ідентифікацію Підписувача (Створювача електронної печатки) шляхом установлення особи за паспортом громадянина України та звірення паспортних даних зі збереженими в реєстрі Підписувачів (Створювачів електронної печатки).

За умови позитивного результату ідентифікації оператор реєстрації передає заяву адміністратору реєстрації. Адміністратор реєстрації за допомогою ПЗ формує запит про блокування сертифіката передає його до КНЕДП.

Обробка заяви в паперовій формі про блокування сертифіката здійснюється протягом не більше ніж дві години з моменту подання заяви.

Адміністратор реєстрації, як і оператор реєстрації, може проводити процедури з ідентифікації та реєстрації заяви.

4.20.5. Блокування сертифіката за зверненням керівництва установи, до якої належить Підписувач

Звернення керівництва установи, до якої належить Підписувач, подається письмово до КНЕДП (ВПР) у довільній формі.

Звернення про блокування сертифіката виконується на бланку установи та повинно бути підписане власноручно керівником такого підрозділу (у тому числі кадрового) із зазначенням обставин, які викликають необхідність блокування, та долученням належним чином засвідчених копій відповідних документів.

Такими обставинами можуть бути:

- тимчасове відсторонення від посади чи виконання службових обов'язків;
- затримання або обрання запобіжного заходу у вигляді тримання під вартою чи цілодобового домашнього арешту;
- тривале відрядження чи його продовження без можливості Підписувачу самотійно звернутися до КНЕДП (ВПР);
- тривала хвороба чи стаціонарне лікування;
- набрання законної сили рішенням суду про блокування кваліфікованого сертифіката відкритого ключа;
- інші причини, які обмежують використання Підписувачем особистого ключа та не дають йому можливості самотійно здійснити блокування сертифіката.

Подання звернення в паперовій формі про блокування сертифіката та його розгляд здійснюються тільки в робочий час відповідно до розпорядку роботи КНЕДП (ВПР).

Під час отримання звернення адміністратор реєстрації перевіряє повноваження керівника та проводить ідентифікацію Підписувача шляхом звірення даних зі збереженими в реєстрі Підписувачів.

За умови позитивного результату ідентифікації адміністратор реєстрації за допомогою ПТК формує запит на блокування сертифіката передає його до КНЕДП.

Обробка такого звернення про блокування сертифіката здійснюється протягом не більше ніж дві години з моменту подання.

4.20.6. Блокування сертифіката за зверненням керівництва установи, до якої належить представник Створювача електронної печатки

Звернення керівництва установи, до якої належить представник Створювача електронної печатки, подається письмово до КНЕДП (ВІПР) у довільній формі.

Звернення про блокування сертифіката виконується на бланку установи та повинно бути підписане власноручно керівником такого підрозділу (у тому числі кадрового) із зазначенням обставин, які викликають необхідність блокування, та долученням належним чином засвідчених копій відповідних документів.

Такими обставинами можуть бути:

- тимчасове припинення використання електронної печатки;
- тимчасове відсторонення від посади чи виконання службових обов'язків працівника, відповідального за її використання;
- інші причини, які обмежують використання Створювачем електронної печатки особистого ключа.

Подання звернення в паперовій формі про блокування сертифіката та його розгляд здійснюються тільки в робочий час відповідно до розпорядку роботи КНЕДП (ВІПР).

Під час отримання звернення адміністратор реєстрації перевіряє повноваження керівника та проводить ідентифікацію Створювача електронної печатки шляхом звірення даних зі збереженими в реєстрі Створювачів електронної печатки.

За умови позитивного результату ідентифікації адміністратор реєстрації за допомогою ПТК формує запит на блокування сертифіката передає його до КНЕДП.

Обробка такого звернення про блокування сертифіката здійснюється протягом не більше ніж дві години з моменту подання.

4.20.7. Блокування сертифіката за повідомленням контролюючого органа чи на підставі судового рішення

Повідомлення контролюючого органа про підозру в компрометації особистого ключа користувача електронних довірчих послуг надходить письмово до КНЕДП (ВІПР) у довільній формі.

Повідомлення виконується на бланку контролюючого органа, повинно містити визначені законодавством обов'язкові реквізити (номер, дата, підпис тощо) та зазначенням обставин, які викликають необхідність блокування. До повідомлення долучаються належним чином засвідчених копій відповідних документів (за наявності).

Рішення суду про блокування кваліфікованого сертифіката відкритого ключа, яке набрало законної сили, надходить письмово до КНЕДП (ВІПР) та має

бути належним чином оформлене, відповідно до вимог Інструкції з діловодства в місцевих та апеляційних судах України, затвердженої наказом Державної судової адміністрації України від 20.08.2019 № 814.

Надходження повідомлення чи судового рішення та його розгляд здійснюються тільки в робочий час відповідно до розпорядку роботи КНЕДП (ВІР).

Під час отримання повідомлення чи судового рішення адміністратор реєстрації перевіряє отримані документи та проводить ідентифікацію користувача електронних довірчих послуг, щодо якого надійшла інформація, шляхом звірення даних зі збереженими в реєстрі Підписувачів (Створювачів електронної печатки).

За умови позитивного результату ідентифікації адміністратор реєстрації за допомогою ПТК формує запит на блокування сертифіката передає його до КНЕДП.

Обробка такого повідомлення чи судового рішення про блокування сертифіката здійснюється протягом не більше ніж дві години з моменту подання.

4.20.8. Порядок скасування сертифікатів

Операція «Скасування» припиняє дію сертифіката. **Скасовані сертифікати поновленню не підлягають.**

Для скасування сертифіката Підписувач (Створювач електронної печатки) подає заяву про скасування до КНЕДП (ВІР) (додаток № 3 до Регламенту).

Скасування сертифіката здійснюється КНЕДП на підставі заяви, що надходить в установленому порядку до КНЕДП (ВІР) або черговому адміністратору реєстрації в усній або паперовій формі.

Заява про скасування сертифіката подається до КНЕДП (ВІР) за відповідною формою, яка доступна на інформаційному ресурсі КНЕДП, і засвідчується підписом власника сертифіката.

Часом скасування сертифіката вважається час внесення інформації про зміну статусу сертифіката до СВС.

4.20.9. Скасування сертифіката за заявою в усній формі

Заява про скасування в усній формі подається адміністратору реєстрації чи черговому адміністратору реєстрації за телефоном.

Підписувач (Створювач електронної печатки) повинен повідомити відповідній посадовій особі КНЕДП таку інформацію:

- своє прізвище, ім'я та по батькові;
- ключову фразу-пароль.

Заява в усній формі приймається тільки при збігу даних Підписувача (Створювача електронної печатки) та фрази-пароля, переданих у заяві, з інформацією, що знаходиться в реєстрі Підписувачів (Створювачів електронної печатки).

Приймання та обробка усної заяви здійснюються у робочий час відповідною особою КНЕДП (ВІР) та цілодобово черговим адміністратором реєстрації. Обробка усної заяви про скасування сертифіката здійснюється безпосередньо після приймання заяви.

Черговий адміністратор реєстрації (адміністратор реєстрації) після перевірки повідомлених даних за допомогою ПТК формує запит на скасування сертифіката з вказанням часу скасування та передає його до КНЕДП.

Обробка заяви про скасування сертифіката здійснюється протягом не більше ніж дві години з моменту подання заяви.

Підписувач (Створювач електронної печатки) не має права використовувати особистий ключ для накладення КЕП, сертифікат ключа якого скасовано.

Часом скасування сертифіката вважається час зміни статусу сертифіката та занесення до СВС.

4.20.10. Скасування сертифіката за заявою в паперовій формі

Заява в паперовій формі подається до КНЕДП (ВІР) за відповідною формою (додаток № 3 до Регламенту).

Заява про скасування сертифіката засвідчується власноручним підписом власника сертифіката.

Подання заяви в паперовій формі про скасування сертифіката та її розгляд здійснюються тільки в робочий час відповідно до розпорядку роботи КНЕДП (ВІР).

Під час приймання заяви оператор реєстрації чи адміністратор реєстрації КНЕДП проводить ідентифікацію Підписувача (Створювача електронної печатки) шляхом установлення особи за паспортом громадянина України та звірення паспортних даних зі збереженими в реєстрі Підписувачів (Створювачів електронної печатки).

За умови позитивного результату ідентифікації оператор реєстрації передає заяву адміністратору реєстрації. Адміністратор реєстрації за допомогою ПЗ формує запит на скасування сертифіката з вказанням часу скасування та передає його до КНЕДП.

Обробка заяви в паперовій формі про скасування сертифіката здійснюється протягом не більше ніж дві години з моменту подання заяви.

Підписувач (Створювач електронної печатки) не має права використовувати особистий ключ для накладення КЕП, сертифікат ключа якого скасовано.

Часом скасування сертифіката вважається час зміни статусу сертифіката та занесення до СВС.

Адміністратор реєстрації, як і оператор реєстрації, може проводити процедури з ідентифікації та реєстрації заяви.

4.20.11. Скасування сертифіката за зверненням керівництва установи, до якої належить Підписувач

Звернення керівництва установи, до якої належить Підписувач, подається письмово до КНЕДП (ВІПР) у довільній формі.

Звернення про скасування сертифіката виконується на бланку та повинно бути підписане власноручно керівником такого підрозділу (у тому числі кадрового) із зазначенням обставин, які викликають необхідність скасування сертифіката, та долученням належним чином засвідчених копій відповідних документів.

Такими обставинами можуть бути:

- смерть Підписувача;
- набрання законної сили рішенням суду про оголошення його померлим, визнання його безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності;
- припинення діяльності відповідного органу чи його підрозділу;
- тривале відсторонення від посади чи виконання службових обов'язків;
- звільнення після затримання, обрання запобіжного заходу у вигляді тримання під вартою чи цілодобового домашнього арешту, засудження до покарання, пов'язаного з позбавленням/обмеженням волі;
- тривале закордонне відрядження чи його продовження без можливості Підписувачу самостійно звернутися до КНЕДП (ВІПР);
- інші причини, які унеможливають використання Підписувачем особистого ключа та самостійне скасування сертифіката.

Подання звернення в паперовій формі про скасування сертифіката та його розгляд здійснюються тільки в робочий час відповідно до розпорядку роботи КНЕДП (ВІПР).

Під час отримання звернення адміністратор реєстрації перевіряє повноваження керівника та проводить ідентифікацію Підписувача шляхом звірення даних зі збереженими в реєстрі Підписувачів.

У випадку надання Підписувачу у користування носія ключової інформації такий носій має бути повернутий до КНЕДП (ВІПР).

За умови позитивного результату ідентифікації адміністратор реєстрації за допомогою ПТК формує запит на скасування сертифіката та передає його до КНЕДП.

Обробка такого звернення про скасування сертифіката здійснюється протягом не більше ніж дві години з моменту подання.

4.20.12. Скасування сертифіката за зверненням керівництва установи, до якої належить представник Створювача електронної печатки

Звернення керівництва установи, до якої належить представник Створювача електронної печатки, подається письмово до КНЕДП (ВІР) у довільній формі.

Звернення про скасування сертифіката виконується на бланку та повинно бути підписане власноручно керівником такого підрозділу (у тому числі кадрового) із зазначенням обставин, які викликають необхідність скасування сертифіката, та долученням належним чином засвідчених копій відповідних документів.

Такими обставинами можуть бути:

- припинення діяльності відповідного органу чи його підрозділу;
- припинення використання електронної печатки;
- звільнення з посади чи зміна уповноваженого працівника, відповідального за її використання (без можливості передати саму електронну печатку);
- набрання законної сили рішенням суду про скасування кваліфікованого сертифіката відкритого ключа електронної печатки;
- інші причини, які унеможливають використання представником Створювача електронної печатки особистого ключа.

Подання звернення в паперовій формі про скасування сертифіката та його розгляд здійснюються тільки в робочий час відповідно до розпорядку роботи КНЕДП (ВІР).

Під час отримання звернення адміністратор реєстрації перевіряє повноваження керівника та проводить ідентифікацію Створювача електронної печатки шляхом звірення даних зі збереженими в реєстрі Створювачів електронної печатки.

У випадку надання Створювачу електронної печатки у користування носія ключової інформації такий носій має бути повернутий до КНЕДП (ВІР).

За умови позитивного результату ідентифікації адміністратор реєстрації за допомогою ПТК формує запит на скасування сертифіката та передає його до КНЕДП.

Обробка такого звернення про скасування сертифіката здійснюється протягом не більше ніж дві години з моменту подання.

4.20.13. Скасування сертифіката за повідомленням контролюючого органа чи на підставі судового рішення

Повідомлення контролюючого органа про факт компрометації особистого ключа користувача електронних довірчих послуг, виявлений під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, надходить письмово до КНЕДП (ВІР) у довільній формі.

Повідомлення виконується на бланку контролюючого органа, повинно містити визначені законодавством обов'язкові реквізити (номер, дата, підпис тощо) та зазначенням обставин, які викликають необхідність скасування. До повідомлення долучаються належним чином засвідчених копій відповідних документів (за наявності).

Рішення суду про скасування кваліфікованого сертифіката відкритого ключа, оголошення Підписувача померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності, визнання користувача електронних довірчих послуг банкрутом, яке набрало законної сили, надходить письмово до КНЕДП (ВІР) та має бути належним чином оформлене, відповідно до вимог Інструкції з діловодства в місцевих та апеляційних судах України, затвердженої наказом Державної судової адміністрації України від 20.08.2019 № 814.

Надходження повідомлення чи судового рішення та його розгляд здійснюються тільки в робочий час відповідно до розпорядку роботи КНЕДП (ВІР).

Під час отримання повідомлення чи судового рішення адміністратор реєстрації перевіряє отримані документи та проводить ідентифікацію користувача електронних довірчих послуг, щодо якого надійшла інформація, шляхом звірення даних зі збереженими в реєстрі Підписувачів (Створювачів електронної печатки).

За умови позитивного результату ідентифікації адміністратор реєстрації за допомогою ПТК формує запит на скасування сертифіката передає його до КНЕДП.

Обробка такого повідомлення чи судового рішення про скасування сертифіката здійснюється протягом не більше ніж дві години з моменту подання.

4.20.14. Порядок поновлення чинності сертифікатів

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

Поновлення чинності сертифіката здійснюється КНЕДП на підставі заяви, яку Підписувач (Створювач електронної печатки) особисто подає до КНЕДП (ВІР) у випадку, якщо блокування відбувалося за заявою Підписувача (Створювача електронної печатки).

Поновлення чинності сертифіката здійснюється КНЕДП на підставі заяви, що надходить в установленому порядку до КНЕДП (ВПР) або черговому адміністратору реєстрації.

4.20.15. Поновлення чинності сертифіката за заявою в усній формі

Заява в усній формі подається черговому адміністратору реєстрації за телефоном.

Підписувач (Створювач електронної печатки) повинен повідомити відповідній посадовій особі КНЕДП таку інформацію:

- своє прізвище, ім'я та по батькові;
- ключову фразу-пароль.

Заява в усній формі приймається тільки при збігу даних Підписувача (Створювача електронної печатки) та фрази-пароля, переданих у заяві, з інформацією, що знаходиться в реєстрі Підписувачів (Створювачів електронної печатки).

Приймання та обробка усної заяви здійснюються у робочий час відповідною особою КНЕДП (ВПР) або цілодобово черговим адміністратором реєстрації. Обробка усної заяви про поновлення чинності сертифіката здійснюється безпосередньо після приймання заяви.

Черговий адміністратор реєстрації після перевірки повідомлених даних за допомогою ПТК формує запит на поновлення сертифіката та передає його до КНЕДП.

4.20.16. Поновлення чинності сертифіката за заявою в паперовій формі

Заява в паперовій формі подається до КНЕДП (ВПР) за відповідною формою (додаток № 3 до Регламенту).

Заява про поновлення чинності сертифіката засвідчується власноручним підписом власника сертифіката.

Подання заяви про поновлення чинності сертифіката та її розгляд здійснюються тільки в робочий час відповідно до розпорядку роботи КНЕДП (ВПР).

Під час приймання заяви оператор реєстрації чи адміністратор реєстрації КНЕДП проводить ідентифікацію Підписувача (Створювача електронної печатки) шляхом установлення особи за паспортом громадянина України та звірення паспортних даних зі збереженими в реєстрі Підписувачів (Створювачів електронної печатки).

За умови позитивного результату ідентифікації оператор реєстрації передає заяву адміністратору реєстрації. Адміністратор реєстрації за допомогою ПЗ формує запит на поновлення чинності сертифіката з вказанням терміну поновлення та передає його до КНЕДП.

Обробка заяви в паперовій формі про поновлення чинності сертифіката здійснюється протягом не більше ніж дві години з моменту подання заяви.

Адміністратор реєстрації, як і оператор реєстрації, може проводити процедури з ідентифікації та реєстрації заяви.

4.20.17. Поновлення чинності сертифіката за зверненням керівництва установи, до якої належить Підписувач (Створювач електронної печатки)

Поновлення чинності сертифіката здійснюється КНЕДП на підставі звернення від керівництва підрозділу, до якого належить Підписувач (Створювач електронної печатки) (у тому числі кадрового), із зазначенням обставин, які викликають необхідність поновлення сертифіката, та долученням належним чином засвідчених копій відповідних документів (у тому числі рішенням суду про поновлення кваліфікованого сертифіката відкритого ключа, яке набрало законної сили).

Подання звернення про поновлення чинності сертифіката та його розгляд здійснюються тільки в робочий час відповідно до розпорядку роботи КНЕДП (ВІР).

Під час приймання заяви оператор реєстрації чи адміністратор реєстрації КНЕДП проводить ідентифікацію Підписувача (Створювача електронної печатки) шляхом установлення особи за паспортом громадянина України та звірення даних зі збереженими в реєстрі Підписувачів (Створювачів електронної печатки).

За умови позитивного результату ідентифікації оператор реєстрації передає заяву адміністратору реєстрації. Адміністратор реєстрації за допомогою ПТК формує запит на поновлення сертифіката та передає його до КНЕДП.

Обробка заяви про поновлення чинності сертифіката повинна здійснюватися протягом не більше ніж дві години з моменту подання.

Адміністратор реєстрації, як і оператор реєстрації, може проводити процедури з ідентифікації та реєстрації заяви чи звернення.

Часом поновлення чинності сертифіката вважається час виключення сертифіката Підписувача (Створювача електронної печатки) зі СВС.

4.20.18. Поновлення чинності сертифіката за повідомленням контролюючого органа чи на підставі судового рішення

Повідомлення контролюючого органа про встановлення недостовірності інформації щодо факту компрометації особистого ключа користувача електронних довірчих послуг, подається письмово тим контролюючим органом, який раніше повідомляв про цю підозру, до КНЕДП (ВІР) у довільній формі.

Повідомлення виконується на бланку контролюючого органа, повинно містити визначені законодавством обов'язкові реквізити (номер, дата, підпис

тощо) та зазначенням обставин, які викликають необхідність поновлення. До повідомлення долучаються належним чином засвідчених копій відповідних документів (за наявності).

Рішення суду про поновлення кваліфікованого сертифіката відкритого ключа, яке набрало законної сили, надходить письмово до КНЕДП (ВІР) та має бути належним чином оформлене, відповідно до вимог Інструкції з діловодства в місцевих та апеляційних судах України, затвердженої наказом Державної судової адміністрації України від 20.08.2019 № 814.

Надходження повідомлення чи судового рішення та його розгляд здійснюються тільки в робочий час відповідно до розпорядку роботи КНЕДП (ВІР).

Під час отримання повідомлення чи судового рішення адміністратор реєстрації перевіряє отримані документи та проводить ідентифікацію користувача електронних довірчих послуг, щодо якого надійшла інформація, шляхом звірення даних зі збереженими в реєстрі Підписувачів (Створювачів електронної печатки).

За умови позитивного результату ідентифікації адміністратор реєстрації за допомогою ПТК формує запит на поновлення сертифіката передає його до КНЕДП.

Обробка такого повідомлення чи судового рішення про поновлення сертифіката здійснюється протягом не більше ніж дві години з моменту подання.

4.21. Порядок надання Надавачем інформації про статус сертифіката

Розповсюдження інформації про статус кваліфікованих сертифікатів електронного підпису чи печатки користувачів здійснюється шляхом публікації повного та часткового списків відкликаних сертифікатів на офіційному веб-сайті надавача та забезпечення створення можливості перевірки статусу кваліфікованого сертифіката електронного підпису чи печатки користувача в режимі реального часу через комунікаційні мережі загального користування.

При використанні Підписувачем (Створювачем електронної печатки) особистого ключа для формування КЕП він повинен попередньо перевірити чинність відповідного цьому ключу сертифіката. Те саме стосується і сертифікатів, які Підписувач (Створювач електронної печатки) або інший користувач використовує для перевірки КЕП.

Для перевірки статусу сертифікатів використовуються такі механізми:

- подання до КНЕДП запитів та отримання відповідей за протоколом OCSP;
- перевірка наявності сертифіката у поточному СВС КНЕДП.

4.21.1. Отримання статусу сертифіката за допомогою OCSP

Взаємодія з КНЕДП за протоколом OCSP дозволяє отримувати інформацію про статус сертифіката в реальному часі. Обмін із Надавачем таким чином здійснюється ПЗ посадових осіб КНЕДП або прикладним ПЗ, що надається Підписувачам (Створювачам електронної печатки), наприклад прикладним застосуванням «Персональний сервіс довірчих послуг».

OCSP-сервер, який функціонує в складі ПТК КНЕДП, має власний ключ КЕП та відповідний йому сертифікат, доступ до якого надається через веб-сайт Надавача.

Для перевірки відповідей OCSP-сервера під час введення в дію сертифіката Підписувача (Створювача електронної печатки) ПЗ записує до особистого контейнера Підписувача (Створювача електронної печатки) ланцюжок сертифікатів, включаючи сертифікати КНЕДП та OCSP-сервера. Крім того, ПЗ може отримувати сертифікати з LDAP-каталогу КНЕДП.

ПЗ Підписувача (Створювача електронної печатки) відправляє запит до OCSP-сервера автоматично щоразу, як проводиться автентифікація користувача, накладення чи перевірка КЕП.

Відповідь від OCSP-сервера приймається і обробляється прикладним ПЗ Підписувача (Створювача електронної печатки) автоматично. Вона містить інформацію про статус сертифіката, щодо якого проводився запит, чи є він чинним, блокованим чи скасованим. Залежно від статусу ПЗ дозволяє або забороняє вхід до системи та/або накладення КЕП, або повідомляє про результат перевірки КЕП.

4.21.2. Отримання статусу сертифіката за допомогою CVC

CVC утримують перелік сертифікатів, що мають статус блокованих та скасованих. CVC формуються Надавачом, засвідчуються КЕП КНЕДП та публікуються в LDAP-каталозі та на веб-сайті КНЕДП. Період публікації становить дві години.

Перевірка статусу сертифіката за допомогою CVC є альтернативою перевірці за протоколом OCSP.

Перевірка статусу за CVC виконується ПЗ посадових осіб та прикладним ПЗ Підписувачів (Створювачів електронної печатки).

За наявності підключення до мережі Internet на робочому місці Підписувача (Створювача електронної печатки) ПЗ автоматично перевіряє актуальність CVC та у разі необхідності завантажує оновлений з LDAP-каталогу чи веб-сайту КНЕДП.

У разі відсутності на робочому місці Підписувача (Створювача електронної печатки) підключення до мережі Internet відповідальність за

наявність актуального СВС покладається на Підписувача (Створювача електронної печатки), який використовує ключі КЕП.

Використання КЕП без перевірки статусу сертифікатів за актуальним СВС чи за OCSP забороняється.

СВС КНЕДП оновлюється при кожному додаванні або виключенні з нього інформації про зміну статусу сертифіката.

4.22. Строк закінчення дії кваліфікованого сертифіката відкритого ключа Підписувача (Створювача електронної печатки)

Строк дії кваліфікованого сертифіката відкритого ключа Підписувача (Створювача електронної печатки) становить не більше двох років.

Початком строку дії особистого ключа Підписувача (Створювача електронної печатки) є дата та час початку дії сертифіката, зазначені у сертифікаті.

Строк дії особистого та відкритого ключа дорівнює строку чинності відповідного сертифіката ключа.

Після закінчення строку чинності сертифіката ключа він вилучається з інформаційного ресурсу КНЕДП та переміщується до архіву.

Після перевершення дати та часу закінчення строку дії кваліфікованого сертифіката Підписувача (Створювача електронної печатки) кваліфікований сертифікат вважається нечинним, а КЕП, накладений із використанням такого особистого ключа Підписувача (Створювача електронної печатки), кваліфікований сертифікат якого нечинний, – недійсним.

КНЕДП зберігає сертифікат та пов'язані з ним СВС безстроково. За запитом користувачів КНЕДП надає доступ до необхідного сертифіката та пов'язаних з ним СВС з архівних записів КНЕДП.

5. Опис процедур та процесів, які виконуються під час надання кваліфікованих електронних довірчих послуг, що не передбачають формування та обслуговування кваліфікованих сертифікатів відкритих ключів

5.1. Надання засобів кваліфікованого електронного підпису чи печатки

Для надання кваліфікованих ЕДП Надавачем використовуються засоби кваліфікованого електронного підпису чи печатки, які мають чинний позитивний експертний висновок за результатами їх державної експертизи у сфері КЗІ.

Засоби КЕП надаються Надавачем у вигляді апаратно-програмних засобів, окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків.

Надання Надавачем засобів КЕП у вигляді окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків, може здійснюватися шляхом передачі цих засобів на носіях інформації (або доступів до багатокористувацьких засобів КЕП) безпосередньо Підписувачу (Створювачу електронної печатки) або шляхом надання доступу через офіційний інформаційний ресурс Надавача, або завдяки сервісам Надавача.

Надавач забезпечує надання Користувачам ЕДП засобів КЕП для створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки шляхом надання доступу до сервісів Надавача через офіційний веб-сайт Надавача.

5.2. Надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу

Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження кваліфікованої електронної позначки часу надається Підписувачам (Створювачам електронних печатки) при створенні КЕП.

Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу Підписувачам (Створювачам електронних печатки) при створенні КЕП надається цілодобово та включає:

- формування кваліфікованої електронної позначки часу;
- передачу кваліфікованої електронної позначки часу користувачеві електронної довірчої послуги.

Кваліфікована електронна позначка часу має презумпцію точності дати та часу, на які вона вказує, та цілісності електронних даних, з якими ці дата та час пов'язані.

Формування та перевірка кваліфікованої електронної позначки часу здійснюється з використанням засобів КЕП.

Перевірка кваліфікованої електронної позначки часу може проводитися будь-яким Користувачем з метою отримання інформації про чинність кваліфікованої електронної позначки часу.

Під час перевірки та підтвердження кваліфікованої електронної позначки часу особа, що проводить перевірку, вчиняє такі дії:

1) отримує з кваліфікованої електронної позначки часу інформацію, що містить ідентифікаційні дані особи, які дають змогу однозначно встановити Надавача;

2) перевіряє КЕП, накладений на кваліфіковану електронну позначку часу за допомогою чинного (на момент формування кваліфікованої електронної позначки часу) кваліфікованого сертифіката Надавача;

3) перевіряє відповідність кваліфікованої електронної позначки часу та електронних даних, до яких вона додана.

Кваліфікована електронна позначка часу вважається недійсною у разі:

1) недотримання вимоги щодо точності часу в ПТК Надавача;

2) використання скасованого або блокованого кваліфікованого сертифіката Надавача на момент формування кваліфікованої електронної позначки часу.

Порядок синхронізації часу із Всесвітнім координованим часом (UTC) погоджується Надавачем із Центральним засвідчувальним органом.

Перелік змін до Регламенту

ЗАЯВА
на проведення реєстрації та формування кваліфікованого сертифіката відкритого ключа
електронного підпису

Заповнюється українською мовою та приймається до розгляду,
якщо немає виправлень, дописок чи необумовлених зауважень (заповнення олівцем не допускається)

Дані Підписувача для формування кваліфікованого сертифіката відкритого ключа електронного підпису			
Назва організації			
Прізвище			
Ім'я			
По батькові			
Посада*			
Роль в ЄРДР**			
Реєстраційний номер облікової картки платника податків			
серія та номер паспорта/номер ID- картки			
Засоби зв'язку (заповнюються обов'язково)			
Телефон +38			E-mail:
Ключова фраза голосової автентифікації			
Згода підписувача на оброблення персональних даних ***			ТАК ☐ НІ ☐
* – вказується посада (індекс підрозділу) відповідно до наказу про призначення (обов'язково для доступу в ЄРДР). ** - відповідно до ст. 3 КПК України (обов'язково для доступу в ЄРДР). *** – Підписувач надає КНЕДП ОПУ згоду на оброблення (збирання, накопичення, зберігання) своїх персональних даних, зазначених у цій заяві та інших документах (заявах), які передбачені Регламентом КНЕДП ОПУ та необхідні для реєстрації його як Підписувача і формування кваліфікованого сертифіката.			
Підписавши цю Заяву, Ви засвідчуєте повне розуміння Регламенту КНЕДП ОПУ, значень термінів і всіх умов. Підписавши цю Заяву, Ви підтверджуєте достовірність та правильність зазначеної в ній інформації, погоджуєтесь на формування кваліфікованого сертифіката відкритого ключа за вказаними даними та зобов'язуєтесь негайно повідомляти про зміну даних, зазначених у цій Заяві.			
Дата	Підпис Підписувача	Прізвище, ініціали Підписувача	
« ____ » _____ 20__ р.			
Даний блок заповнюється адміністратором реєстрації			
Адміністратор реєстрації _____ / _____ / _____ датапідписПІБ			

ЗАЯВА
на проведення реєстрації та формування кваліфікованого сертифіката відкритого ключа
електронної печатки

Заповнюється українською мовою та приймається до розгляду,
якщо немає виправлень, дописок чи необумовлених зауважень (заповнення олівцем не допускається)

Дані Створювача для формування кваліфікованого сертифіката відкритого ключа електронної печатки									
<i>Назва організації</i>									
Код ЄДРПОУ									
Найменування печатки									
Відомості про уповноважену посадову особу, відповідальну за застосування електронної печатки									
Прізвище									
Ім'я									
По батькові									
Посада									
Засоби зв'язку (заповнюються обов'язково)									
Телефон +38	0					E-mail:			
Ключова фраза голосової автентифікації									
<i>Згода уповноваженої особи Створювача на оброблення персональних даних *</i>							<i>Відтиск печатки</i>		
ТАК ☐ НІ ☐									
* – Уповноважена особа надає КНЕДП ОПУ згоду на оброблення (збирання, накопичення, зберігання) своїх персональних даних, зазначених у цій заяві та інших документах (заявах), які передбачені Регламентом КНЕДП ОПУ та необхідні для реєстрації Створювача електронної печатки і формування кваліфікованого сертифіката. Підписавши цю Заяву, Ви засвідчуєте повне розуміння Регламенту КНЕДП ОПУ, значень термінів і всіх умов. Підписавши цю Заяву, Ви підтверджуєте достовірність та правильність зазначеної в ній інформації, погоджуєтесь на формування кваліфікованого сертифіката відкритого ключа за вказаними даними та зобов'язуєтесь негайно повідомляти про зміну даних, зазначених у цій Заяві.									
<i>Дата</i>	<i>Підпис Уповноваженої особи</i>				<i>Прізвище, ініціали Уповноваженої особи</i>				
« ____ » _____ 20__ р.	_____				_____				
Даний блок заповнюється адміністратором реєстрації									
Адміністратор реєстрації _____ / _____ / _____									
дата підпис ПІБ									

ЗАЯВА
про зміну статусу кваліфікованого сертифіката відкритого ключа електронного підпису чи
електронної печатки

Заповнюється українською мовою та приймається до розгляду,
якщо немає виправлень, дописок чи необумовлених зауважень (заповнення олівцем не допускається)

Дані Підписувача (Створювача електронної печатки), які були зазначені при формуванні кваліфікованого сертифіката																																	
<i>Назва організації</i>																																	
<i>Код ЄДРПОУ*</i>	<table border="1" style="width: 100%; height: 20px;"><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>																																
<i>Прізвище</i>																																	
<i>Ім'я</i>																																	
<i>По батькові</i>																																	
<i>Посада**</i>																																	
<i>Реєстраційний номер облікової картки платника податків</i>	<table border="1" style="width: 100%; height: 20px;"><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>																<i>серія та номер паспорта/номер ID-картки</i>	<table border="1" style="width: 100%; height: 20px;"><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>															
Зміна статусу кваліфікованого сертифіката (оберіть один із варіантів)																																	
<table style="width: 100%;"><tr><td style="border: 1px solid black; padding: 5px; display: inline-block;">Скасувати</td><td style="border: 1px solid black; width: 20px; height: 20px; display: inline-block;"></td><td style="border: 1px solid black; padding: 5px; display: inline-block; margin: 0 10px;">Заблокувати</td><td style="border: 1px solid black; width: 20px; height: 20px; display: inline-block;"></td><td style="border: 1px solid black; padding: 5px; display: inline-block;">Поновити</td><td style="border: 1px solid black; width: 20px; height: 20px; display: inline-block;"></td></tr></table>				Скасувати		Заблокувати		Поновити																									
Скасувати		Заблокувати		Поновити																													
<i>Причина скасування кваліфікованого сертифіката електронного підпису чи електронної печатки (заповнюється обов'язково у разі необхідності скасування кваліфікованого сертифіката):</i>																																	
<i>Підписавши цю Заяву, Ви підтверджуєте достовірність та правильність зазначеної вище інформації.</i>																																	
<i>Дата</i>	<i>Підпис</i>	<i>Прізвище, ініціали</i>																															
«_____» _____ 20____ р.	_____	_____																															
*- обов'язково заповнюється при скасуванні електронної печатки **- заповнюється за наявності у сертифікаті																																	
Даний блок заповнюється адміністратором реєстрації																																	
<i>Адміністратор реєстрації</i>	/	/	/																														
_____	_____	_____	_____																														
дата	підпис		ПІБ																														