Додаток 1

до Регламенту роботи кваліфікованого надавача електронних довірчих послуг – акредитованого центру сертифікації ключів Міністерства внутрішніх справ України

**ПОЛІТИКА СЕРТИФІКАТА**

кваліфікованого надавача електронних довірчих послуг – акредитованого центру сертифікації ключів Міністерства внутрішніх справ України

# ЗМІСТ

# 1. ВСТУП

## 1.1. Огляд

Ця Політика сертифіката кваліфікованого надавача електронних довірчих послуг – акредитованого центру сертифікації ключів Міністерства внутрішніх справ України (далі – Політика сертифіката) визначає перелік усіх правил, що застосовуються кваліфікованим надавачем електронних довірчих послуг – акредитованим центром сертифікації ключів Міністерства внутрішніх справ України (далі - КНЕДП – АЦСК МВС) у процесі реєстрації КЕД послуг, зокрема, реєстрації заявників, підписувачів, створювачів електронних печаток, які на підставі договору отримують КЕД послуги в КНЕДП – АЦСК МВС (далі - користувачі), формування та обслуговування кваліфікованих сертифікатів відкритих ключів (далі - кваліфіковані сертифікати) КНЕДП – АЦСК МВС та користувачів, а також управління їх статусом (блокування, поновлення та скасування).

Дотримання вимог, визначених у цій Політиці сертифіката, є обов'язковим для працівників КНЕДП – АЦСК МВС, посадові обов'язки яких безпосередньо пов'язані з реєстрацією користувачів, формуванням та обслуговуванням їхніх кваліфікованих сертифікатів, у тому числі для працівників ВПР КНЕДП – АЦСК МВС.

Визнання користувачами вимог, визначених у цій Політиці сертифіката, є обов'язковою умовою та підставою для укладення з ними Договору про надання кваліфікованих електронних довірчих послуг (договір приєднання) (далі – Договір про надання КЕД послуг).

Перелік усіх практичних дій та процедур, що застосовуються для реалізації КНЕДП – АЦСК МВС цієї Політики сертифіката, визначають Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг – акредитованого центру сертифікації ключів Міністерства внутрішніх справ України щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до Регламенту) (далі - Положення сертифікаційних практик).

Ця Політика сертифіката відповідає вимогам, визначеним у:

- ДСТУ ETSI EN 319 411-1 (ETSI EN 319 411-1) "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги" (далі - ДСТУ ETSI EN 319 411-1);

- ДСТУ ETSI EN 319 411-2 (ETSI EN 319 411-2) "Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС" (далі - ДСТУ ETSI EN 319 411-2);

- ДСТУ ETSI EN 319 412-2 (ETSI EN 319 412-2, IDT) "Електронні підписи та інфраструктури. (ESI). Профілі сертифікатів. Частина 2. Профілі сертифікатів, виданих фізичним особам" (далі - ДСТУ ETSI EN 319 412-2);

- ДСТУ ETSI EN 319 401 (ETSI EN 319 401, IDT) "Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг" (далі - ДСТУ ETSI EN 319 401).

## 1.2. Назва документа та його ідентифікація

Назва документа та його ідентифікація визначається відповідно до положень пункту 5.3 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

Повна назва документа: Політика сертифіката надавача електронних довірчих послуг – акредитованого центру сертифікації ключів Міністерства внутрішніх справ України.

Скорочена назва документа: Політика сертифіката.

Версія: 1.0.

Об'єктний ідентифікатор (OID) Політики сертифіката: 1.2.804.2.1.1.1.2.

Об'єктний ідентифікатор (OID) Політики сертифіката присвоєно відповідно до стандарту ASN.1 згідно з вмістом наведеної нижче таблиці. Таблиця 1. Структура об'єктного ідентифікатора (OID) Політики сертифіката

| Опис | Скорочена назва | Значення (індекс) |
|---|---|---|
| Ознака першої гілки (дуги) кореневого вузла світового дерева об'єктних ідентифікаторів (OID), що знаходиться в підпорядкуванні вузла Міжнародної організації стандартизації (ISO) | iso | 1 |
| Ознака національного органу стандартизації, що є членом Міжнародної організації стандартизації (ISO) | member-body | 2 |
| Унікальний числовий код України відповідно до ДСТУ ISO 3166-1:2009 «Коди назв країн світу» (ISO 3166-1:2006, IDT), затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 23 грудня 2009 р. № 471 (далі - ISO 3166-1) | ua | 804 |
| Ознака інфраструктури відкритих ключів | root; security; cryptography; uapki | 2.1.1.1 |
| Ознака політики сертифікації | cp | 2 |

Кваліфіковані сертифікати, сформовані КНЕДП – АЦСК МВС, містять об'єктний ідентифікатор (OID) цієї Політики сертифіката, який використовується суб'єктами, які довіряють КНЕДП – АЦСК МВС, для визначення придатності та надійності таких сертифікатів під час автентифікації користувачів, зокрема шляхом перевірки та підтвердження кваліфікованого електронного підпису чи печатки.

### 1.3. Учасники інфраструктури відкритих ключів

До учасників інфраструктури відкритих ключів, зазначених у цьому розділі застосовуються вимоги, визначені в пункті 5.4 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411- 2.

#### 1.3.1. КНЕДП – АЦСК МВС

КНЕДП – АЦСК МВС є кваліфікованим надавачем електронних довірчих послуг (далі - КНЕДП), що надає КЕД послуги з дотриманням вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (далі - Закон), зокрема, здійснює реєстрацію користувачів, формування та обслуговування їхніх кваліфікованих сертифікатів, у тому числі, управління їхнім статусом (блокування, поновлення та скасування).

КНЕДП – АЦСК МВС здійснює реєстрацію користувачів самостійно та/або через ВПР КНЕДП – АЦСК МВС.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

##### 1.3.1.1. Права КНЕДП – АЦСК МВС

Права КНЕДП визначено у статті 13 Закону.

КНЕДП – АЦСК МВС має право:

надавати КЕД послуги з дотриманням вимог законодавства у сфері електронних довірчих послуг;

отримувати документи та/або електронні дані, необхідні для ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті;

проводити під час формування та видачі кваліфікованих сертифікатів перевірку інформації про осіб, яким видаються такі сертифікати, з використанням відомостей інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ України (відомостей щодо викрадених (втрачених) документів за зверненнями 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 відповідно до Порядку проведення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи - підприємця під час надання електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 28 червня 2024 р. № 764;

отримувати консультації від ЦЗО, контролюючого органу з питань, пов’язаних з наданням КЕД послуг;

звертатися до органів з оцінки відповідності для отримання документів про відповідність;

звертатися до ЦЗО із заявами про формування кваліфікованих сертифікатів, їх скасування, блокування або поновлення;

самостійно обирати в рамках кожної послуги, які саме стандарти вони будуть застосовувати для надання КЕД послуг з переліку стандартів, визначеного Кабінетом Міністрів України.

### 1.3.1.2. Обов’язки КНЕДП – АЦСК МВС

Обов’язки кваліфікованих надавачів електронних довірчих послуг визначено у статті 13 Закону. КНЕДП – АЦСК МВС зобов’язаний забезпечувати:

захист персональних даних користувачів відповідно до вимог Закону України «Про захист персональних даних»;

функціонування ІКС та ПТК, що використовуються для надання КЕД послуг, та захист інформації, яка обробляється в них, відповідно до вимог законодавства у сфері електронних довірчих послуг;

створення та функціонування свого веб-сайту;

впровадження, підтримання в актуальному стані та публікацію на своєму веб-сайті відомостей з реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

можливість цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус кваліфікованих сертифікатів через комунікаційні мережі загального користування;

цілодобовий прийом та перевірку заяв користувачів в електронній формі заяв про скасування, блокування та поновлення їхніх кваліфікованих сертифікатів;

прийом та перевірку заяв користувачів у паперовій формі заяв про скасування, блокування та поновлення їхніх кваліфікованих сертифікатів протягом одного робочого дня після надходження заяви та згідно з режимом роботи КНЕДП – АЦСК МВС;

скасування, блокування та поновлення кваліфікованих сертифікатів відповідно до вимог Закону;

встановлення під час формування кваліфікованого сертифіката належності відкритого ключа та відповідного йому особистого ключа користувачу;

внесення даних користувача до відповідного кваліфікованого сертифіката;

вжиття організаційних і технічних заходів з управління ризиками, пов'язаними з безпекою КЕД послуг;

інформування контролюючого органу та, в разі необхідності, органу з питань захисту персональних даних про порушення конфіденційності та/або цілісності інформації, що впливають на надання КЕД послуг або стосуються персональних даних Користувачів, без необґрунтованої затримки, не пізніше ніж протягом 24 годин з моменту, коли стало відомо про таке порушення;

інформування користувачів про порушення конфіденційності та/або цілісності інформації, що впливають на надання їм КЕД послуг або стосуються їхніх персональних даних, без необґрунтованої затримки, але не пізніше двох годин з моменту, коли стало відомо про таке порушення;

унеможливлення використання особистого ключа Користувача, якщо стало відомо про компрометацію такого особистого ключа та якщо особистий ключ Користувача зберігається у КНЕДП – АЦСК МВС у межах надання послуги створення, перевірки та підтвердження КЕП;

постійне зберігання всіх виданих кваліфікованих сертифікатів відкритих ключів;

постійне зберігання документів та електронних даних, отриманих у зв'язку з наданням електронних довірчих послуг відповідно до переліку, встановленого Кабінетом Міністрів України;

внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) для забезпечення відшкодування шкоди, яка може бути завдана Користувачам чи третім особам внаслідок неналежного виконання КНЕДП – АЦСК МВС своїх зобов'язань, або страхування цивільно-правової відповідальності для забезпечення відшкодування такої шкоди у розмірі, визначеному Законом;

відновлення розміру внеску на поточному рахунку із спеціальним режимом використання у банку (на рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або розміру страхової суми, що встановлені Законом, протягом трьох місяців у разі зміни розміру мінімальної заробітної плати або в разі відшкодування збитків, завданих Користувачам чи третім особам внаслідок неналежного виконання своїх зобов'язань;

використання під час надання КЕД послуг виключно кваліфікованих сертифікатів, сформованих ЦЗО;

наймання працівників та, за потреби, виконання робіт субпідрядними організаціями, які володіють необхідними для надання КЕД послуг знаннями, досвідом і кваліфікацією, та застосування адміністративних і управлінських процедур, які відповідають національним або міжнародним стандартам;

чітке та вичерпне повідомлення будь-якій особі, яка звернулася за отриманням КЕД послуг, про умови використання такої послуги, у тому числі про будь-які обмеження її використання, перед укладенням Договору про надання КЕД послуг;

інформування контролюючого органу та ЦЗО про намір припинити свою діяльність та про зміни у наданні КЕД послуг протягом 48 годин з моменту настання таких змін;

передачу ЦЗО або іншому КНЕДП документованої інформації в разі припинення діяльності з надання КЕД послуг;

приєднання до програмного інтерфейсу ІКС ЦЗО з метою забезпечення інтероперабельності, дослідження поточного стану, перспектив розвитку сфери КЕД послуг.

### 1.3.2. Органи реєстрації

КНЕДП – АЦСК МВС, ВПР КНЕДП – АЦСК МВС є органами реєстрації, до складу яких входять працівники Департаменту інформатизації Міністерства внутрішніх справ України, територіальних органів МВС, підрозділів центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України, закладів, установ чи підприємств, що належать до сфер їх управління, а також юридичних осіб, які на підставі наказу або договору з МВС здійснюють реєстрацію користувачів.

До працівників відокремлених пунктів реєстрації КНЕДП – АЦСК МВС, на яких покладено обов'язки з реєстрації користувачів, застосовуються такі ж вимоги, як і до адміністраторів реєстрації, що визначені у пункті 5.3.1.2 цієї Політики сертифіката. Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 1.3.3. Користувачі

Користувачами є підписувачі та створювачі електронних печаток, щодо яких КНЕДП – АЦСК МВС здійснює їх реєстрацію (самостійно або через ВПР КНЕДП – АЦСК МВС), формування та обслуговування їхніх кваліфікованих сертифікатів відкритих ключів.

Права та обов'язки користувачів визначені у статті 12 Закону.

Відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги»:

- підписувач – це фізична особа, яка створює електронний підпис;

- створювач електронної печатки - юридична особа або фізична особа - підприємець, яка створює електронну печатку.

### 1.3.3.1. Права користувачів

Користувачі мають право на:

- отримання КЕД послуг;

- вільний вибір КНЕДП;

- оскарження у судовому порядку дій чи бездіяльності КНЕДП – АЦСК МВС та органів, що здійснюють державне регулювання у сфері електронних довірчих послуг;

- відшкодування завданої їм шкоди та захист своїх прав і законних інтересів;

- звернення із заявою про скасування, блокування та поновлення свого кваліфікованого сертифіката;

- вільне використання результатів отриманих КЕД послуг з урахуванням обмежень, встановлених законодавством та КНЕДП– АЦСК МВС.

Отримуючи КЕД послуги в КНЕДП – АЦСК МВС користувач має право:

- одержувати кваліфіковані сертифікати КНЕДП – АЦСК МВС;

- одержувати кваліфіковані сертифікати користувачів у разі надання ними згоди на публікацію або використання їх сертифікатів;

- одержувати списки відкликаних сертифікатів, сформованих КНЕДП – АЦСК МВС;

- застосовувати списки відкликаних сертифікатів, сформованих КНЕДП – АЦСК МВС, та протокол інтерактивного визначення статусу сертифіката (OCSP) для перевірки статусу кваліфікованого сертифіката, сформованого КНЕДП – АЦСК МВС;

- застосовувати кваліфікований сертифікат КНЕДП – АЦСК МВС для перевірки справжності кваліфікованих сертифікатів, сформованих КНЕДП – АЦСК МВС;

- застосовувати список відкликаних сертифікатів, сформованих КНЕДП – АЦСК МВС, та протокол інтерактивного визначення статусу сертифіката (OCSP) для перевірки статусу кваліфікованих сертифікатів користувачів;

- використовувати засоби КЕП, надані КНЕДП – АЦСК МВС, для перевірки КЕП;

- отримувати консультації з питань роботи КНЕДП – АЦСК МВС та порядку надання ним КЕД послуг;

- ознайомлюватись з інформацією щодо діяльності КНЕДП – АЦСК МВС та надання ним КЕД послуг, зокрема на офіційному веб-сайті КНЕДП – АЦСК МВС.

### 1.3.3.2. Обов’язки користувачів

Користувачі зобов'язані:

- виконувати вимоги Регламенту, Політики сертифіката, положень сертифікаційних практик в частині, що їх стосуються;

- забезпечувати конфіденційність та неможливість доступу інших осіб до

особистого ключа;

- невідкладно повідомляти КНЕДП – АЦСК МВС про підозру або факт компрометації особистого ключа;

- надавати достовірну інформацію, необхідну для отримання КЕД послуг;

- своєчасно надавати КНЕДП – АЦСК МВС інформацію про зміну ідентифікаційних даних, які містить кваліфікований сертифікат;

- не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування кваліфікованого сертифіката;

- здійснювати перевірку КЕП відповідно до статті 18 Закону;

- враховувати визначені у кваліфікованих сертифікатах вимоги щодо сфери та обмежень їх використання.

### 1.3.4. Суб'єкти, які довіряють КНЕДП – АЦСК МВС

Фізичні та юридичні особи, а також їхні інформаційно-комунікаційні системи є суб'єктами, які довіряють КНЕДП – АЦСК МВС, та використовують кваліфіковані сертифікати користувачів з метою їх автентифікації, зокрема шляхом перевірки та підтвердження КЕП.

### 1.3.5. Інші учасники

Фізичні та юридичні особи, які прямо чи опосередковано пов'язані з формуванням та/або обслуговування кваліфікованих сертифікатів КНЕДП – АЦСК МВС та користувачів, є іншими учасниками.

До інших учасників належать також ЦЗО та контролюючий орган, які є наглядовими органами щодо КНЕДП – АЦСК МВС.

ЦЗО, зокрема:

- погоджує Регламент, цю Політику сертифіката та відповідні Положення сертифікаційних практик, зміни до них, а також направляє їхні копії до КО;

- погоджує порядок синхронізації часу із Всесвітнім координованим часом (UTC) КНЕДП – АЦСК МВС;

- погоджує План припинення діяльності КНЕДП – АЦСК МВС.

Контролюючий орган (Адміністрація Державної служби спеціального зв'язку та захисту інформації України), зокрема:

- здійснює державний контроль за дотриманням вимог законодавства у сфері електронних довірчих послуг;

- взаємодіє з ЦЗО та органами з оцінки відповідності з питань державного контролю за дотриманням вимог законодавства;

- співпрацює з органами з питань захисту персональних даних шляхом невідкладного інформування про порушення вимог законодавства про захист персональних даних, виявлені під час проведення контролюючим органом перевірок КНЕДП – АЦСК МВС;

- інформує громадськість у разі отримання від КНЕДП – АЦСК МВС або за результатами його перевірки, відомостей про порушення конфіденційності та/або цілісності інформації, що впливають на надання КЕД послуг або стосуються персональних даних користувачів;

- видає приписи щодо усунення порушень вимог законодавства у сфері електронної ідентифікації та електронних довірчих послуг;

- накладає адміністративні штрафи за порушення вимог законодавства у сфері електронної ідентифікації та електронних довірчих послуг;

- аналізує документи про відповідність за результатами проведення процедур оцінки відповідності КНЕДП – АЦСК МВС у рамках невиїзних заходів державного нагляду (контролю).

Також до інших учасників належить адміністратор інформаційно-комунікаційної системи ЦЗО, який забезпечує виконання, зокрема, таких функцій:

- ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів, які сформовані ЦЗО;

- надання КЕД послуг КНЕДП – АЦСК МВС з використанням самопідписаного сертифіката електронної печатки ЦЗО, що призначений для надання таких послуг;

- надання послуги з постачання передачі сигналів точного часу, синхронізованого з Державним еталоном одиниць часу і частоти;

- приймання та зберігання документованої інформації, сформованих кваліфікованих сертифікатів, відомостей з реєстру чинних, блокованих та скасованих кваліфікованих сертифікатів у разі припинення діяльності КНЕДП – АЦСК МВС з надання КЕД послуг.

### 1.4. Використання кваліфікованих сертифікатів

Використання кваліфікованих сертифікатів здійснюється відповідно до положень пункту 5.5 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

#### 1.4.1. Дозволене використання кваліфікованих сертифікатів

##### 1.4.1.1. Види кваліфікованих сертифікатів

КНЕДП – АЦСК МВС формує кваліфіковані сертифікати таких видів:

- кваліфікований сертифікат електронного підпису, що пов’язує відкритий ключ кваліфікованого електронного підпису з фізичною особою та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження кваліфікованого електронного підпису;

- кваліфікований сертифікат електронної печатки, що пов’язує відкритий ключ кваліфікованої електронної печатки з юридичною особою або фізичною особою - підприємцем та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження кваліфікованої електронної печатки;

- кваліфікований сертифікат шифрування, що пов’язує відкритий ключ кваліфікованого електронного підпису чи печатки з фізичною особою, юридичною особою або фізичною особою - підприємцем та забезпечує направлене шифрування під час обміну інформацією.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

##### 1.4.1.2. Строк дії кваліфікованих сертифікатів

Кваліфіковані сертифікати КНЕДП – АЦСК МВС формуються ЦЗО зі строком дії не більше 5 років.

Строк дії кваліфікованих сертифікатів КНЕДП – АЦСК МВС становить:

1. особистого ключа КНЕДП – АЦСК МВС 5 років з параметрами, що відповідають

таким вимогам:

• алгоритм електронного підпису ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», (далі - ДСТУ 4145-2002), розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;

• алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT).

2. CMP 5 років з параметрами, що відповідають таким вимогам:

• алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;

• алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT).

3. TSP 5 років;

4. OCSP 5 років з параметрами, що відповідають таким вимогам:

• алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;

• алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT).

Кваліфіковані сертифікати користувачів формуються КНЕДП – АЦСК МВС зі строком не більше 2 років.

Кваліфіковані сертифікати обов'язково містять відомості про початок та закінчення строку їх дії.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 1.4.2. Обмеження у використанні кваліфікованих сертифікатів

КНЕДП – АЦСК МВС має право встановлювати сфери, в яких дозволяється використовувати кваліфіковані сертифікати, та визначати обмеження щодо використання сформованих ним кваліфікованих сертифікатів. Обмеження щодо використання сформованих КНЕДП – АЦСК МВС кваліфікованих сертифікатів застосовуються відповідно до норм законодавства України.

Для кваліфікованих сертифікатів, сформованих Підписувачам, створювачам електронної печатки – представникам державних установ діють обмеження щодо використання КЕП, установлені Порядком використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затвердженим постанови Кабінету Міністрів України від 01.08.2023 № 798.

Інформація щодо обмеження сфери або сфер використання сертифіката доводиться до користувача та зазначається у сформованому КНЕДП – АЦСК МВС кваліфікованому сертифікаті.

Не допускається використання кваліфікованого сертифіката, сформованого КНЕДП – АЦСК МВС, у сферах, що не відповідають зазначеному у кваліфікованому сертифікаті

призначенню відкритого ключа (“keyUsage”).

### 1.4.3. Використання тестових сертифікатів

Формування тестових сертифікатів здійснюється КНЕДП – АЦСК МВС через інтеграцію з тестовим програмно-технічним комплексом, створеним на офіційному вебсайті ЦЗО в рамках інструменту моніторингу сфери електронних довірчих послуг (https://czo.gov.ua/tool) відповідно до наказу Міністерства цифрової трансформації України від 18.01.2024 № 11 «Про деякі питання діяльності та розвитку у сферах електронної ідентифікації та електронних довірчих послуг», зареєстрованого в Міністерстві юстиції України 05 лютого 2024 р. за № 180/41525.

Склад тестових сертифікатів має чітко вказувати, що вони призначені для цілей тестування (наприклад, за назвою суб’єкта).

Використання тестових сертифікатів обмежується та здійснюється лише з метою перевірки функціональності та тестування.

## 1.5. Керування Політикою сертифіката

### 1.5.1. Відповідальність за Політику сертифіката

Ця Політика сертифікації підтримується КНЕДП – АЦСК МВС, ВПР КНЕДП – АЦСК МВС та користувачами КЕД послуг, що надаються КНЕДП – АЦСК МВС.

Договори про надання КЕД послуг укладаються від імені Міністерства внутрішніх справ України.

Ця Політика сертифіката структурована відповідно до RFC 3647 «Інфраструктура відкритих ключів Інтернету X.509 Політика сертифікатів і практика сертифікації» і містить всю необхідну інформацію.

Ця Політика сертифіката, а також зміни до неї підписується керівником КНЕДП – АЦСК МВС, який відповідає за дотримання, визначених у ній правил, та затверджується Міністром внутрішніх справ України.

Ця Політика сертифіката, а також зміни до неї погоджуються Міністерством цифрової трансформації України, яке направляє її копію до Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

### 1.5.2. Внесення змін до Політики сертифіката

Відповідно до пункту 9.12 цієї Політики сертифіката.

Зміни до Політики сертифіката вносяться у порядку, передбаченому законодавством для внесення змін до Регламенту.

### 1.6. Визначення термінів та перелік скорочень

#### 1.6.1. Визначення термінів

У цій Політиці сертифіката терміни застосовуються у значеннях, наведених у Цивільному кодексі України, Законах України "Про захист інформації в інформаційно-комунікаційних системах", "Про захист персональних даних", "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус", "Про електронні комунікації", "Про електронну ідентифікацію та електронні довірчі послуги", постанові Кабінету міністрів України від 28.06.2024 р. № 764 "Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг" (із змінами), інших нормативно-правових актах у сферах електронних довірчих послуг, криптографічного та технічного захисту інформації, електронних комунікацій.

#### 1.6.2. Перелік скорочень

| | |
|---|---|
| ДРАЦС | Державний реєстр актів цивільного стану громадян |
| ДРФО | Державний реєстр фізичних осіб - платників податків |
| ЄДДР | Єдиний державний демографічний реєстр |
| ЄДР | Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань |
| ЄДРПОУ | Єдиний державний реєстр підприємств та організацій України |
| ЄІС МВС | Єдина інформаційна система Міністерства внутрішніх справ України |
| ІКС | Інформаційно-комунікаційна система |
| КЗІ | Криптографічний захист інформації |
| КО | Контролюючий орган (Адміністрація державної служби спеціального зв'язку та захисту інформації України) |
| ООВ | Орган з оцінки відповідності |
| ПТК | Програмно-технічний комплекс |
| РНОКПП | Реєстраційний номер облікової картки платника податків |
| УНЗР | Унікальний номер запису в ЄДДР |
| ЦЗО | Центральний засвідчувальний орган (Міністерство цифрової трансформації України) |
| CMP | Certificate Management Protocol |

| | |
|---|---|
| CRL | Certificate Revocation List (список відкликаних сертифікатів) |
| OCSP | Online Certificate Status Protocol (протокол визначення статусу сертифіката) |
| TSP | Time Stamp Protocol |

## 2. ОБОВ'ЯЗКИ ЩОДО ПУБЛІКАЦІЇ ТА ЗБЕРІГАННЯ

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги визначені в положеннях пункту 6.1 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

### 2.1. Репозиторій/веб-сайт

КНЕДП – АЦСК МВС повинен забезпечувати:

- створення та функціонування офіційного веб-сайту КНЕДП – АЦСК МВС;

- впровадження, підтримання в актуальному стані та публікацію на веб-сайті КНЕДП – АЦСК МВС відомостей з реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

- можливість цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів відкритих ключів через комунікаційні мережі загального користування.

- інформування користувачів про умови отримання кваліфікованих електронних довірчих послуг шляхом розміщення відповідної інформації на веб-сайті КНЕДП – АЦСК МВС.

На офіційному веб-сайті КНЕДП – АЦСК МВС публікується інформація, передбачена пунктом 35 Вимог до надавачів послуг електронної ідентифікації та електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 28 червня 2024 року № 764 (зі змінами), зокрема така:

- відомості про КНЕДП – АЦСК МВС (у тому числі, про ВПР КНЕДП – АЦСК МВС та виїзних адміністраторів реєстрації);

- дані про внесення відомостей про КНЕДП – АЦСК МВС до Довірчого списку;

- тексти Регламенту,, цієї Політики сертифіката та Положень сертифікаційних практик;

- текст Договору про надання КЕД послуг;

- перелік КЕД послуг, які надає КНЕДП – АЦСК МВС;

- дані про засоби КЕП, що використовуються під час надання КЕД послуг;

- реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів;

- відомості про обмеження під час використання кваліфікованих сертифікатів користувачами;

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

- нормативно-правові акти у сфері надання КЕД послуг;

- кваліфіковані сертифікати ЦЗО;

- кваліфіковані сертифікати КНЕДП – АЦСК МВС, серверів КНЕДП – АЦСК МВС (OCSP, TSP, CMP);

- кваліфіковані сертифікати користувачів, які надали згоду на їх публікацію;

- форми заяв, які подаються до КНЕДП – АЦСК МВС для отримання КЕД послуг, зразки їх заповнення та рекомендації щодо порядку подання таких заяв.

Ця Політика сертифіката доступна на веб-сайті КНЕДП – АЦСК МВС 24 години на добу 7 днів на тиждень у форматі лише для читання та в обсязі положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

КНЕДП – АЦСК МВС забезпечує регулярне оновлення інформації та публікацію кваліфікованих сертифікатів, Регламенту, цієї Політики сертифіката, Положень сертифікаційних практик, списків відкликаних сертифікатів, договорів, актів законодавства та інших нормативних документів на веб-сайті КНЕДП – АЦСК МВС.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 2.2. Публікація інформації

#### 2.2.1. Публікація кваліфікованих сертифікатів користувачів

Кваліфіковані сертифікати користувачів, які надали згоду на їх публікацію, публікуються одразу після формування таких кваліфікованих сертифікатів та виконання користувачами умов Договору про надання КЕД послуг.

Згода на публікацію кваліфікованого сертифіката надається користувачем під час подання заяви щодо формування кваліфікованого сертифіката.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

#### 2.2.2. Публікація сертифікатів КНЕДП – АЦСК МВС

Кваліфіковані сертифікати КНЕДП – АЦСК МВС повинні публікуватися на веб-сайті КНЕДП – АЦСК МВС одразу після їх отримання від ЦЗО.

Кваліфіковані сертифікати серверів КНЕДП – АЦСК МВС публікуються одразу після їх формування КНЕДП – АЦСК МВС.

КНЕДП – АЦСК МВС забезпечує регулярне оновлення інформації та публікацію кваліфікованих сертифікатів, текстів Регламенту, цієї Політики сертифіката, Положень сертифікаційних практик, CRL, договорів, нормативно-правових актів та інших нормативних документів на веб-сайті КНЕДП – АЦСК МВС.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

#### 2.2.3. Доступ до сертифікатів користувачів

Кваліфіковані сертифікати користувача після їх формування КНЕДП – АЦСК МВС повинні бути доступні користувачу, якому такий сертифікат був сформований.

Доступ інших осіб до кваліфікованих сертифікатів користувачів надається за умови надання такими користувачами згоди на їх публікацію.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

#### 2.2.4. Строк закінчення дії сертифіката

Строк дії кваліфікованих сертифікатів користувачів становить не більше двох років. Строк дії кваліфікованих сертифікатів КНЕДП – АЦСК МВС становить:

1. особистого ключа КНЕДП – АЦСК МВС 5 років з параметрами, що відповідають таким вимогам:

- алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;
- алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT).

2. CMP 5 років з параметрами, що відповідають таким вимогам:

- алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;
- алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT).

3. TSP 5 років;
4. OCSP 5 років з параметрами, що відповідають таким вимогам:

- алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;
- алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT).

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 2.3. Час та періодичність публікації

Кваліфіковані сертифікати серверів КНЕДП – АЦСК МВС публікуються одразу після їх формування КНЕДП – АЦСК МВС.

Кваліфіковані сертифікати користувачів, які надали згоду на їх публікацію, публікуються КНЕДП – АЦСК МВС одразу після формування таких сертифікатів.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 2.4. Контроль доступу до репозиторію/веб-сайту

Репозиторій/веб-сайт захищений від несанкціонованого доступу та змін. КНЕДП – АЦСК МВС забезпечує цілодобове функціонування власного репозиторію/веб-сайту.

За захист інформації на репозиторії/веб-сайті та базі даних МВС відповідає служба захисту інформації, визначена відповідно до рішення керівництва МВС та документів щодо КСЗІ в ІКС КНЕДП – АЦСК МВС. Доступ до управління репозиторієм/веб-сайтом та базою даних КНЕДП – АЦСК МВС надано адміністраторам служби захисту інформації КНЕДП – АЦСК МВС.

## 3. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.2 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

### 3.1. Позначення

Кваліфіковані сертифікати обов’язково повинні містити відомості, визначені частиною другою статті 23 Закону.

Кваліфіковані сертифікати можуть містити відомості про обмеження використання КЕП.

Кваліфіковані сертифікати можуть містити інші необов'язкові додаткові спеціальні атрибути, визначені у стандартах для кваліфікованих сертифікатів. Такі атрибути не повинні впливати на інтероперабельність і визнання КЕП.

Відомостям, що містяться в кваліфікованих сертифікатах, відповідають позначення (реквізити, атрибути), визначені в стандартах щодо профілів сертифікатів відповідно до пункту 7.1 цієї Політики сертифіката.

Позначення, що використовуються в кваліфікованих сертифікатах користувачів КНЕДП – АЦСК МВС, наведені в Таблиці 2 Положень сертифікаційних практик.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 3.1.1. Типи позначень кваліфікованих сертифікатів

Типи позначень (реквізитів, атрибутів) кваліфікованого сертифіката, що відповідають відомостям, які містяться в кваліфікованих сертифікатах, визначені в стандартах щодо профілів сертифікатів відповідно до пункту 7.1 цієї Політики сертифіката.

### 3.1.2. Позначення (реквізити та атрибути) кваліфікованих сертифікатів

Кваліфікований сертифікат повинен мати всі необхідні позначення (реквізити, атрибути), визначені в стандартах щодо профілів сертифікатів відповідно до пункту 7.1 розділу 7 цієї Політики сертифіката.

### 3.1.3. Анонімність або використання псевдонімів

Не застосовується.

### 3.1.4. Правила інтерпретації різних форм позначень кваліфікованих сертифікатів

Міжнародні літери повинні кодуватися згідно з UTF-8.

### 3.1.5. Унікальність позначень кваліфікованих сертифікатів

КНЕДП – АЦСК МВС повинен гарантувати, що сертифікати з однаковими даними, зазначеними в полях “Common Name” та “SerialNumber”, не видаються різним користувачам.

### 3.1.6. Визнання, автентифікація та роль торгових марок

Не застосовується.

## 3.2. Первинна перевірка ідентифікації

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.2.2 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

### 3.2.1. Механізм (підтвердження) володіння особистим ключем

Підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката, забезпечується в один із таких способів:

- візуальним та технічним контролем запису та передачі до КНЕДП – АЦСК МВС запиту на формування кваліфікованого сертифіката особисто користувачем під час генерації пари ключів одразу після ідентифікації користувача, за умови його особистої присутності;

- технічним контролем запису та передачі до КНЕДП – АЦСК МВС запиту на формування кваліфікованого сертифіката особисто користувачем під час генерації пари ключів одразу після ідентифікації користувача та отримання ідентифікаційних даних за

допомогою механізмів ідентифікації, зазначених у підпункті 3.2.2 цієї Політики сертифіката, а також відповідних Положень сертифікаційних практик КНЕДП – АЦСК МВС.

У всіх випадках за допомогою засобів кваліфікованого електронного підпису чи печатки КНЕДП – АЦСК МВС здійснюється перевірка удосконаленого електронного підпису, створеного за допомогою особистого ключа користувача на запиті на формування кваліфікованого сертифіката, за допомогою відкритого ключа, що міститься у цьому запиті.

Підтвердження володіння користувачем особистим ключем здійснюється без розкриття особистого ключа.

### 3.2.2. Автентифікація особи

Формування та видача кваліфікованого сертифіката без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті, не допускаються.

Ідентифікація особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката, здійснюється в один із таких способів:

1) за особистої присутності фізичної особи, фізичної особи - підприємця чи уповноваженого представника юридичної особи - за результатами перевірки відомостей (даних) про особу, отриманими у встановленому законодавством порядку з ЄДДР, за паспортом громадянина України або іншими документами, виданими відповідно до законодавства про ЄДДР та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи (паспорт громадянина України, паспорт громадянина України для виїзду за кордон, посвідка на постійне/тимчасове місце проживання);

2) віддалено (без особистої присутності особи), з одночасним використанням засобу електронної ідентифікації, що має високий або середній рівень довіри, раніше виданого фізичній особі, фізичній особі - підприємцю чи уповноваженому представнику юридичної особи за особистої присутності, та багатофакторної автентифікації;

3) за ідентифікаційними даними особи, що містяться у кваліфікованому сертифікаті, раніше сформованому та виданому згідно з підпунктом 1 або 2 цього пункту, за умови чинності такого сертифіката;

4) з використанням інших способів ідентифікації, визначених законом, надійність яких є еквівалентною особистій присутності та підтверджена ООВ.

У разі відсутності в іноземців та осіб без громадянства документів, виданих відповідно до законодавства про ЄДДР та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи, їх ідентифікація у спосіб, визначений підпунктом 1 пункту 3.2.2 цієї Політики сертифіката, здійснюється за легалізованим належним чином паспортним документом іноземця або документом, що посвідчує особу без громадянства.

Під час перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи - підприємця (з метою формування кваліфікованого сертифіката електронної печатки) КНЕДП – АЦСК МВС зобов'язаний використовувати інформацію про юридичну особу чи фізичну особу - підприємця, що міститься в ЄДР або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи, а також пересвідчитися, що обсяг цивільної правоздатності та дієздатності юридичної особи чи фізичної особи - підприємця є достатнім для формування та видачі кваліфікованого сертифіката.

Перевірка цивільної правоздатності та дієздатності міжнародних організацій, відомості про яких не внесені до ЄДР або торговельного, банківського чи судового реєстру, що ведеться іноземною державою, за місцезнаходженням штаб-квартири міжнародної організації здійснюється з використанням інформації з міжнародного договору або іншого офіційного документа, на підставі якого створена та/або діє міжнародна організація.

У випадках передачі обслуговування кваліфікованих сертифікатів користувачів та документованої інформації, на підставі якої були сформовані зазначені сертифікати, від КНЕДП , який припиняє свою діяльність, до КНЕДП – АЦСК МВС процедура ідентифікації цих користувачів проводиться одним із способів зазначених в цьому пункті та відповідно до Закону.

Відповідні Положення сертифікаційних практик КНЕДП – АЦСК МВС містять додаткову інформацію.

### 3.2.3. Неперевірена інформація про користувача

Неперевірена інформація про користувача не допускається.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 3.2.4. Підтвердження повноважень

Уповноважений представник юридичної особи або фізичної особи - підприємця підписує документи, необхідні для формування та видачі кваліфікованого сертифіката працівнику юридичної особи або фізичної особи - підприємця. КНЕДП – АЦСК МВС під час формування та видачі кваліфікованого сертифіката працівнику юридичної особи або фізичної особи - підприємця здійснює ідентифікацію працівника, а також ідентифікацію особи уповноваженого представника юридичної особи або фізичної особи - підприємця здійснює ідентифікацію працівника, відповідно до вимог, встановлених підпунктом 3.2.2 цієї Політики сертифіката та перевіряє обсяг його повноважень за документом, що визначає повноваження уповноваженого представника юридичної особи або фізичної особи - підприємця, чи з використанням інформації, що міститься в ЄДР або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи.

Уповноваженим представником юридичної особи є керівник юридичної особи, який зазначений в ЄДР, або співробітник (керівник відокремленого підрозділу (філії) юридичної особи) наділений повноваженнями укладання правочинів з третіми особами, які зазначаються в наказі, довіреності тощо.

Перед формуванням кваліфікованого сертифіката представника юридичної особи та самозайнятої особи (адвокат, нотаріус, приватний виконавець, арбітражний керуючий тощо) також здійснюється перевірка повноважень користувача шляхом перевірки документів, що засвідчують його повноваження або приналежність до юридичної особи, право на здійснення діяльності у визначеній сфері (посвідчення, сертифікат, наказ про призначення, свідоцтво тощо) або шляхом перевірки інформації у відповідних державних інформаційних системах (реєстри, бази даних тощо).

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 3.3. Ідентифікація та автентифікація за заявою на повторне формування кваліфікованих сертифікатів відкритого ключа

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.2.3 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

### 3.3.1. Ідентифікація та автентифікація користувача за заявою щодо формування повторного сертифіката за умови чинності попереднього сертифіката

Для формування нового кваліфікованого сертифіката користувача, що має чинний кваліфікований сертифікат, сформований КНЕДП – АЦСК МВС, такий користувач проходить процедуру автентифікації за поданою в електронній формі до КНЕДП – АЦСК МВС заявою щодо формування кваліфікованого сертифіката за умови незмінності ідентифікаційних даних, внесених до попереднього кваліфікованого сертифіката, з моменту формування кваліфікованого сертифіката до моменту створення КЕП на заяві про формування кваліфікованого сертифіката.

Перевірка ідентифікаційних даних користувача, який звертається із заявою про формування кваліфікованого сертифіката в електронній формі, а також законності такого звернення, здійснюється шляхом автентифікації користувача та підтвердження його повноважень за результатами перевірки кваліфікованого електронного підпису на заяві та встановленням чинності сертифіката ключа, що містить ідентифікаційні дані особи на момент подання заяви.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 3.3.2. Ідентифікація та автентифікація користувача на отримання повторного кваліфікованого сертифіката у разі скасування сертифіката

У разі, якщо кваліфікований сертифікат користувача скасовано, для формування нового кваліфікованого сертифіката в КНЕДП – АЦСК МВС користувач повинен пройти ідентифікацію та автентифікацію згідно з умовами для первинної ідентифікації та автентифікації користувача.

### 3.4. Ідентифікація та автентифікація користувача за заявами про блокування або скасування сертифіката

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.2.4 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

Для блокування або скасування кваліфікованого сертифіката користувача, що має чинний кваліфікований сертифікат, сформований КНЕДП – АЦСК МВС, такий користувач проходить процедуру автентифікації за поданою до КНЕДП – АЦСК МВС заявою про блокування або скасування кваліфікованого сертифіката.

Пункт 4.9 цієї Політики сертифіката та відповідних Положень сертифікаційних практик містить додаткову інформацію щодо блокування та скасування кваліфікованого сертифіката користувача.

## 4. ВИМОГИ ДО ЖИТТЄВОГО ЦИКЛУ СЕРТИФІКАТА

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

### 4.1. Заява щодо формування кваліфікованого сертифіката

До переліку суб’єктів, уповноважених подавати заяву щодо формування кваліфікованого сертифіката, належать користувачі, що пройшли процедури ідентифікації та автентифікації.

Заява щодо формування кваліфікованого сертифіката приймається в обробку після ідентифікації та автентифікації особи користувача та підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката.

Пункт 4.1 відповідних Положень сертифікаційних практик містять додаткову інформацію щодо процесу реєстрації користувача.

### 4.2. Обробка запиту на формування кваліфікованого сертифіката

До об'єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3.2 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

Обробка запиту на формування кваліфікованого сертифіката здійснюється програмними засобами ІКС КНЕДП – АЦСК МВС за участю адміністратора реєстрації, працівника відокремленого пункту реєстрації КНЕДП – АЦСК МВС, на якого покладено обов'язки з реєстрації користувачів, та який виконує функції адміністратора реєстрації, або автоматично за умови забезпечення безперервності процесів генерації пар ключів, формування запитів, передачі їх на обробку захищеними каналами зв'язку, які забезпечують конфіденційність та цілісність даних. Автоматична обробка запитів не виключає процесів ідентифікації особи користувача та підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката.

Під час обробки запиту на формування кваліфікованого сертифіката засобами ІКС КНЕДП – АЦСК МВС здійснюється перевірка унікальності відкритого ключа в реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів та забезпечується унікальність серійного номера кваліфікованого сертифіката користувача.

Строк обробки запиту на формування кваліфікованого сертифіката, поданого разом із заявою на реєстрацію, становить не більше двох годин.

### 4.3. Формування сертифіката

Надання сформованого кваліфікованого сертифіката користувачу здійснюється в один із таких способів:

- шляхом запису файлу із сформованим кваліфікованим сертифікатом на носій інформації, наданий користувачем (за бажанням користувача);

- шляхом публікації сформованого кваліфікованого сертифіката на веб-сайті КНЕДП – АЦСК МВС (у випадку надання користувачем згоди на їх публікацію).

### 4.4. Прийняття сертифіката

До об'єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3.4 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

Кваліфікований сертифікат користувача публікується на веб-сайті КНЕДП – АЦСК МВС одразу після його формування.

Користувач повинен протягом доби перевірити свої ідентифікаційні дані, внесені КНЕДП – АЦСК МВС до кваліфікованого сертифіката. КНЕДП – АЦСК МВС повинен надавати відповідні консультації щодо проведення такої перевірки. Користувач повинен використовувати особистий ключ для створення кваліфікованого електронного підпису тільки після проведення перевірки. Використання користувачем особистого ключа є фактом визнання ним кваліфікованого сертифіката, що відповідає його відкритому ключу.

Перевірка працездатності свого особистого ключа та ідентифікаційних даних внесених до кваліфікованого сертифіката здійснюється користувачем за результатом пошуку та подальшого завантаження кваліфікованих сертифікатів на веб-сайті КНЕДП – АЦСК МВС (https://ca.mvs.gov.ua/certificates-search) або за допомогою програмного комплексу

«Користувач АЦСК МВС», що доступне для завантаження на веб-сайті КНЕДП – АЦСК МВС за посиланням https://ca.mvs.gov.ua/user-downloads.

У разі виявлення користувачем протягом однієї доби невідповідності ідентифікаційних даних, внесених КНЕДП – АЦСК МВС до кваліфікованого сертифіката, користувач повинен звернутися до КНЕДП – АЦСК МВС для скасування кваліфікованих сертифікатів та формування нових.

У разі невідповідності ідентифікаційних даних, внесених КНЕДП – АЦСК МВС до кваліфікованих сертифікатів та виявлених КНЕДП – АЦСК МВС до моменту надання сформованих кваліфікованих сертифікатів користувачу, працівником КНЕДП – АЦСК МВС здійснюється переформування кваліфікованих сертифікатів із використанням попередньо засвідченого відкритого ключа та з дотриманням вимог щодо недопущення перевищення часу чинності особистого ключа та відповідного йому відкритого ключа більше двох років. Працівник, що здійснив переформування кваліфікованих сертифікатів, складає акт, у якому зазначається дата та час скасування кваліфікованих сертифікатів та формування нових, ідентифікаційні дані користувача, що містяться в кваліфікованому сертифікаті та невідповідні ідентифікаційні дані користувача, що зазначені у заяві щодо формування кваліфікованого сертифіката. Акт підписується працівником КНЕДП – АЦСК МВС та реєстратором сертифікації, що здійснив переформування кваліфікованого сертифіката, та долучається до документів (засвідчених в установленому порядку копій документів), що використовувалися під час встановлення особи та реєстрації користувача.

### 4.5. Використання пари ключів і сертифіката

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3.5 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

#### 4.5.1. Використання особистого ключа та кваліфікованих сертифікатів користувачем

Користувач зобов'язаний дотримуватися таких правил під час використання особистого ключа:

забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;

невідкладно повідомляти КНЕДП – АЦСК МВС про підозру або факт компрометації особистого ключа;

не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування відповідних кваліфікованих сертифікатів;

особисто відповідати за захист паролю від особистого ключа.

Користувач зобов’язаний використовувати кваліфікований сертифікат відповідно до зазначеного у ньому призначення відкритого ключа (“keyUsage”) та обмежень щодо його використання.

Під час використання особистого ключа та кваліфікованих сертифікатів користувач повинен дотримуватися вимог законодавства у сфері електронних довірчих послуг, а також положень:

- Регламенту, цієї Політики сертифіката, Положень сертифікаційних практик;

- Договору про надання КЕД послуг.

### 4.5.2. Використання відкритого ключа та кваліфікованих сертифікатів суб'єктами, які довіряють КНЕДП – АЦСК МВС

Кваліфіковані сертифікати користувачів, сформовані КНЕДП – АЦСК МВС, можуть використовуватися будь-якими суб'єктами, які довіряють КНЕДП – АЦСК МВС, з метою їх автентифікації, зокрема шляхом перевірки та підтвердження електронного підпису чи печатки.

Перш ніж прийняти КЕП користувача, суб'єкт, який довіряє КНЕДП – АЦСК МВС, повинен перевірити таку інформацію:

- статус кваліфікованого сертифіката користувача, сферу використання кваліфікованого сертифіката користувача, обмеження використання та інформацію про кваліфікований сертифікат користувача.

- відповідність особистого ключа КЕП відкритому ключу зазначеному в кваліфікованому сертифікаті користувача.

Суб'єкт, який довіряє КНЕДП – АЦСК МВС, повинен виконати такі перевірки:

- перевірити статус кваліфікованого сертифіката користувача на момент накладання КЕП за допомогою OCSP-серверу КНЕДП – АЦСК МВС (сервер перевірки статусу кваліфікованого сертифіката), сферу використання (поле KeyUsage в сертифікаті), обмеження використання та інформацію про кваліфікований сертифікат, щоб переконатися, що кваліфікований сертифікат користувача чинний в даний момент;

- перевірити статус кваліфікованого сертифіката КНЕДП – АЦСК МВС під час накладання кваліфікованого електронного підпису чи печатки користувачем.

КЕП вважається дійсними, коли здійснені результати перевірки в наведених вище пунктах виконані успішно та є дійсними одночасно.

Суб'єкт, який довіряє КНЕДП – АЦСК МВС, несе відповідальність за те, що не дотримувався вищевказаної процедури перевірки або виконував перевірку, знаючи, що кваліфікований сертифікат не чинний на момент перевірки.

Під час використання відкритого ключа та кваліфікованого сертифіката користувача суб'єкти, які довіряють КНЕДП – АЦСК МВС, повинні дотримуватися вимог законодавства у сфері електронних довірчих послуг, а також положень Регламенту, цієї Політики сертифіката та Положень сертифікаційних практик.

### 4.6. Поновлення сертифіката

До об'єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3.6 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

КНЕДП – АЦСК МВС забезпечує, зокрема:

- цілодобовий прийом та перевірку заяв в електронній формі користувачів на поновлення їхніх кваліфікованих сертифікатів, які були заблоковані КНЕДП – АЦСК МВС;

- прийом та перевірку заяв у паперовій формі користувачів на поновлення кваліфікованих сертифікатів користувачів, які були заблоковані КНЕДП – АЦСК МВС, протягом одного робочого дня після надходження заяви та згідно з режимом роботи КНЕДП – АЦСК МВС електронних довірчих послуг не пізніше ніж протягом двох годин після надходження заяви та згідно з режимом роботи КНЕДП – АЦСК МВС, ВПР КНЕДП – АЦСК МВС;

- поновлення кваліфікованих сертифікатів, які були заблоковані КНЕДП – АЦСК МВС, відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 4.7. Повторне формування сертифіката

До об'єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3.7 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

КНЕДП – АЦСК МВС здійснює формування кваліфікованого сертифіката користувача, у тому числі на підставі чинного кваліфікованого сертифіката, сформованого КНЕДП – АЦСК МВС, що містить ідентифікаційні дані користувача, отримані за результатами його ідентифікації в один із таких способів:

- за особистої присутності фізичної особи, фізичної особи - підприємця чи уповноваженого представника юридичної особи – за результатами перевірки відомостей (даних) про особу, отриманими у встановленому законодавством порядку з ЄДДР, за паспортом громадянина України або іншими документами, виданими відповідно до законодавства про ЄДДР та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи;

- віддалено (без особистої присутності особи), з одночасним використанням засобу електронної ідентифікації, що має високий рівень довіри, раніше виданого фізичній особі, фізичній особі - підприємцю чи уповноваженому представнику юридичної особи за особистої присутності, та багатофакторної автентифікації.

КНЕДП – АЦСК МВС також формує нові кваліфіковані сертифікати користувачів у випадку закінчення строку їх дії та у разі нагальної потреби (компрометації особистого ключа чи паролю до нього, втрати особистого ключа, зміни відомостей, що містяться у кваліфікованих сертифікатах користувача тощо) за зверненням користувачів.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 4.8. Зміна сертифіката

Внесення змін до кваліфікованого сертифіката не допускається.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 4.9. Скасування та блокування кваліфікованих сертифікатів

До об'єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.3.9 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

КНЕДП – АЦСК МВС забезпечує, зокрема:

- цілодобовий прийом та перевірку заяв в електронній формі користувачів про скасування, блокування та поновлення їхніх кваліфікованих сертифікатів, сформованих КНЕДП – АЦСК МВС;

- прийом та перевірку заяв у паперовій формі користувачів про скасування, блокування та поновлення їхніх кваліфікованих сертифікатів, сформованих КНЕДП – АЦСК МВС, протягом одного робочого дня після надходження заяви та згідно з режимом роботи КНЕДП – АЦСК МВС;

- скасування, блокування та поновлення кваліфікованих сертифікатів, сформованих КНЕДП – АЦСК МВС, відповідно до вимог Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

Користувач має право за власним бажанням здійснити блокування кваліфікованого сертифіката. Блокування кваліфікованого сертифіката може здійснюватися КНЕДП – АЦСК МВС за паперовою заявою про зміну статусу кваліфікованого сертифіката або за усною заявою після ідентифікації користувача за ключовою фразою, внесеною до заяви про реєстрацію. Під блокуванням кваліфікованого сертифіката розуміється тимчасове призупинення чинності кваліфікованого сертифіката строком до 30 календарних днів.

Після блокування кваліфікованого сертифіката, користувач може протягом 30 календарних днів поновити чинність кваліфікованих сертифікатів. Блокований кваліфікований сертифікат буде автоматично скасовано, якщо протягом зазначеного строку користувач не поновить його чинність.

Кваліфікований сертифікат втрачає чинність з моменту зміни його статусу на "скасований". Скасований кваліфікований сертифікат поновленню не підлягає.

Кваліфікований сертифікат вважається заблокованим з моменту зміни його статусу на "заблокований". Кваліфікований сертифікат, статус якого змінено на "заблокований", у період блокування є нечинним та не використовується.

КНЕДП – АЦСК МВС формує списки відкликаних сертифікатів (CRL) у вигляді повного та часткового списків, які відповідають таким вимогам:

- у кожному списку відкликаних сертифікатів зазначається граничний строк його дії до видання нового списку;

- новий список відкликаних сертифікатів може бути опубліковано до настання граничного строку його дії до видання наступного списку;

- на список відкликаних сертифікатів повинен бути накладений КЕП КНЕДП – АЦСК МВС.

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

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

Посилання на списки відкликаних сертифікатів вносяться до кваліфікованих сертифікатів користувачів.

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

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

Відповідні Положення сертифікаційних практик КНЕДП – АЦСК МВС містять додаткову інформацію.

### 4.10. Служби статусу сертифіката

КНЕДП – АЦСК МВС забезпечує доступність інформації про статус сертифіката в реальному часі за допомогою OCSP-серверу та списків відкликаних сертифікатів (CRL), що публікуються на веб-сайті КНЕДП – АЦСК МВС.

### 4.11. Закінчення строку дії сертифіката

Дата та час початку та закінчення строку дії сертифіката користувача зазначається у сертифікаті із точністю до однієї секунди.

Після настання дати та часу закінчення строку дії сертифіката користувача, зазначеного в ньому, такий сертифікат вважається скасованим.

### 4.12. Депонування та повернення ключів

Не застосовується.

## 5. ОБ'ЄКТ, УПРАВЛІННЯ ТА ОПЕРАЦІЙНИЙ КОНТРОЛЬ

До об'єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пунктах 5, 6.3 і 7.3 ДСТУ ETSI EN 319 401.

### 5.1. Контроль фізичної безпеки

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

## 5.2. Процедурний контроль

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 5.3. Контроль працівників КНЕДП – АЦСК МВС

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 5.4. Архів документів

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 5.5. Зміна ключа

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 5.6. Компрометація і аварійне відновлення

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 5.7. Припинення діяльності КНЕДП – АЦСК МВС

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.4.9 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2. Припинення діяльності КНЕДП – АЦСК МВС проводиться відповідно до затвердженого Плану припинення діяльності з надання кваліфікованих електронних довірчих послуг (далі - План припинення діяльності) з урахуванням вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

#### 5.7.1. Підстави припинення діяльності КНЕДП – АЦСК МВС

КНЕДП – АЦСК МВС припиняє свою діяльність з надання КЕД послуг у разі:

1) прийняття ЦЗО рішення про скасування статусу КНЕДП;

2) прийняття КНЕДП – АЦСК МВС рішення про припинення надання усіх КЕД послуг, що зазначені у Довірчому списку;

3) припинення діяльності КНЕДП – АЦСК МВС (припинення юридичної особи), крім випадків правонаступництва, визначених 5.7.4 цієї Політики сертифіката);

4) набрання законної сили рішенням суду про скасування статусу кваліфікованого надавача, визнання КНЕДП – АЦСК МВС банкрутом.

Про рішення щодо припинення надання КЕД послуг КНЕДП – АЦСК МВС зобов'язаний повідомити користувачів, ЦЗО та КО не пізніше п'яти робочих днів з дати прийняття такого рішення.

З дати оприлюднення ЦЗО на своєму офіційному веб-сайті повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП – АЦСК МВС та до дати припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП – АЦСК МВС зобов'язаний надавати електронні довірчі послуги, крім формування нових кваліфікованих сертифікатів.

КНЕДП – АЦСК МВС, припиняючи діяльність з надання кваліфікованих електронних довірчих послуг, передає іншому КНЕДП обслуговування користувачів, з якими ним було укладено договори про надання кваліфікованих електронних довірчих послуг.

У разі припинення надання кваліфікованих довірчих послуг КНЕДП – АЦСК МВС зобов'язаний передати іншому КНЕДП або ЦЗО документовану інформацію (документи, на підставі яких користувачам надавалися кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані кваліфіковані сертифікати, усі сформовані кваліфіковані сертифікати, а також реєстри сформованих кваліфікованих сертифікатів).

Передача документованої інформації буде здійснена КНЕДП – АЦСК МВС не пізніше дати, визначеної ним як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, або дати набрання законної сили відповідним рішенням суду.

ЦЗО скасовує виданий ним кваліфікований сертифікат КНЕДП – АЦСК МВС в день, визначений КНЕДП – АЦСК МВС як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, або в день набрання законної сили рішенням відповідного суду.

### 5.7.2. Повідомлення про припинення діяльності КНЕДП – АЦСК МВС

Про прийняте рішення про припинення надання кваліфікованих електронних довірчих послуг КНЕДП – АЦСК МВС зобов'язаний повідомити користувачам, ЦЗО та КО не пізніше п'яти робочих днів з дня прийняття такого рішення.

ЦЗО зобов'язаний оприлюднити інформацію про рішення ЦЗО щодо припинення КНЕДП – АЦСК МВС діяльності з надання кваліфікованих електронних довірчих послуг, в тому числі у зв'язку із скасуванням статусу КНЕДП, не пізніше наступного робочого дня після прийняття такого рішення шляхом:

- розміщення інформації про таке рішення на своєму офіційному веб-сайті;

- надіслання до КНЕДП – АЦСК МВС повідомлення про таке рішення із зазначенням підстави його прийняття.

ЦЗО зобов'язаний опублікувати на своєму офіційному веб-сайті повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП – АЦСК МВС не пізніше наступного робочого дня з дня одержання повідомлення про настання підстав, передбачених підпунктами 2 - 4 пункту 5.7.1 цієї Політики сертифіката.

Повідомлення ЦЗО про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП – АЦСК МВС повинно містити дату опублікування.

### 5.7.3. Дата припинення діяльності КНЕДП – АЦСК МВС

КНЕДП – АЦСК МВС припиняє свою діяльність з надання КЕД послуг через три місяці з дня опублікування на офіційному веб-сайті ЦЗО повідомлення про припинення надання КЕД послуг КНЕДП – АЦСК МВС .

З дня опублікування на офіційному веб-сайті ЦЗО повідомлення про припинення діяльності з надання КЕД послуг КНЕДП – АЦСК МВС та до дня припинення діяльності з надання КЕД послуг КНЕДП – АЦСК МВС зобов'язаний надавати електронні довірчі послуги, крім формування нових кваліфікованих сертифікатів.

ЦЗО у день, визначений як дата припинення діяльності КНЕДП – АЦСК МВС з надання КЕД послуг, вносить відповідні зміни до Довірчого списку.

### 5.7.4. Правонаступництво

З метою забезпечення безперервного надання КЕД послуг їх користувачам ЦЗО може прийняти рішення про внесення змін до Довірчого списку щодо заміни КНЕДП шляхом заміни відомостей про КНЕДП – АЦСК МВС відомостями про іншого КНЕДП, якщо передача відповідних прав та обов'язків здійснюється за спільною згодою таких КНЕДП, за договором або з інших підстав для правонаступництва, визначених законодавством.

Порядок внесення змін до Довірчого списку щодо заміни КНЕДП, а також особливості набуття та скасування статусу КНЕДП у разі заміни КНЕДП визначаються Порядком ведення Довірчого списку, затвердженим наказом Міністерства цифрової трансформації України 08 липня 2020 року № 104, зареєстрованим в Міністерстві юстиції України 29 липня 2020 р. за № 719/35002.

### 5.7.5. Передача документованої інформації

КНЕДП – АЦСК МВС у разі припинення діяльності з надання КЕД послуг, зобов'язаний передати до іншого КНЕДП, який виявив намір продовжити обслуговування користувачів до закінчення строку дії відповідних Договорів про надання КЕД послуг, або до ЦЗО документи, на підставі яких користувачам надавалися кваліфіковані електронні довірчі послуги та були сформовані, блоковані, поновлені, скасовані кваліфіковані сертифікати, усі сформовані кваліфіковані сертифікати, а також реєстри сформованих кваліфікованих сертифікатів.

Передача документованої інформації здійснюється відповідно до:

- Порядку передачі обслуговування користувачів електронних довірчих послуг, з якими кваліфікований надавач електронних довірчих послуг, що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, уклав договори про надання КЕД послуг, до іншого кваліфікованого надавача електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 23 липня 2024 р. № 842;

- Порядку зберігання документованої інформації та її передавання центральному засвідчувальному органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 10 грудня 2024 р. № 1408;

- підпунктів 6.3.4-10A та 6.3.4-11A ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

### 5.7.6. План припинення діяльності

КНЕДП – АЦСК МВС має затверджений План припинення діяльності.

План припинення діяльності визначає умови, яких повинен дотримуватися КНЕДП – АЦСК МВС з метою недопущення негативних наслідків у разі припинення ним діяльності з надання КЕД послуг та забезпечення стабільності та довговічності КЕД послуг.

КНЕДП – АЦСК МВС затверджує План припинення діяльності та за необхідності вносить до нього зміни з метою актуалізації інформації, що в ньому міститься.

ЦЗО погоджує План припинення діяльності та зміни до нього в установленому законодавством порядку.

У Плані припинення діяльності визначаються:

- порядок повідомлення користувачів, ЦЗО, персоналу КНЕДП – АЦСК МВС, ВПР КНЕДП – АЦСК МВС, суб'єктів, які довіряють КНЕДП – АЦСК МВС та контрагентів про припинення діяльності з надання КЕД послуг;

- домовленості та угоди з третіми сторонами для продовження виконання зобов'язань у разі припинення КНЕДП – АЦСК МВС діяльності з надання КЕД послуг (передача обслуговування користувачів до іншого КНЕДП).

План припинення діяльності є конфіденційним і перевіреним ООВ.

## 6. ТЕХНІЧНІ ЗАХОДИ БЕЗПЕКИ

### 6.1. Генерація та встановлення пари ключів

### 6.1.1. Генерація пари ключів

#### 6.1.1.1. Генерація пари ключів КНЕДП – АЦСК МВС

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

#### 6.1.1.5. Генерація пари ключів користувача

Під час генерації ключів користувачів забезпечується наступне:

- використання користувачем виключно засобу КЕП та кваліфікованого сертифіката;

- захист обміну інформацією між користувачем та КНЕДП – АЦСК МВС засобами електронних комунікаційних мереж загального користування;

- створення умов для генерації пари ключів користувача;

- допомога під час генерації пари ключів користувача у спосіб, що не допускає порушення конфіденційності та цілісності особистого ключа, а також ознайомлення із значенням параметрів особистого ключа та їх копіювання;

- унікальність пари ключів користувача;

- захист від доступу сторонніх осіб до параметрів особистого ключа користувача під час використання засобу КЕП.

Особистий та відкритий ключі користувача може бути згенеровано:

– на робочому місці або особистому комп'ютерному обладнанні користувача;
– на робочій станції генерації ключів у КНЕДП – АЦСК МВС, ВПР КНЕДП – АЦСК МВС;
– у суб'єктів, уповноважених на видачу паспорта громадянина України з імплантованим БЕН, які здійснюють представництво КНЕДП – АЦСК МВС, за допомогою засобів робочої станції для оформлення та видачі документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус.

Особистий ключ користувача генерується засобом КЕП та захищається паролем. Відповідальність за забезпечення конфіденційності та цілісності власного особистого ключа несе сам користувач.

Особисті ключі користувачів не зберігаються у КНЕДП – АЦСК МВС.

У разі генерації відкритого та особистого ключів на робочому місці або особистому комп'ютерному обладнанні користувача для ініціювання такої генерації застосовуються засоби КЕП, що надаються КНЕДП – АЦСК МВС.

Запит на сертифікацію подається до КНЕДП – АЦСК МВС в особі адміністратора реєстрації (віддаленого адміністратора реєстрації) на носієві інформації разом із заявою про реєстрацію або у складі відповідної електронної заяви (запиту).

У разі генерації відкритого та особистого ключа користувача у КНЕДП – АЦСК МВС, ВПР КНЕДП – АЦСК МВС, ключі генеруються ним особисто на робочій станції генерації ключів, що входить до складу ІКС КНЕДП – АЦСК МВС.

Для генерації відкритого та особистого ключів на робочій станції генерації ключів, що входить до складу ІКС КНЕДП – АЦСК МВС, на робочому місці або особистому комп'ютерному обладнанні користувача застосовуються засоби КЕП.

Запит на сертифікацію подається до КНЕДП – АЦСК МВС в особі адміністратора реєстрації (віддаленого адміністратора реєстрації) разом із заявою про реєстрацію, на носієві інформації, окремому від носія ключової інформації.

У разі генерації перших пар ключових даних на БЕН, імплантований у паспорт громадянина України, генерація таких пар здійснюється фізичною особою, на ім'я якої оформлено паспорт громадянина України з імплантованим БЕН, у суб'єктів, уповноважених на видачу паспорта громадянина України з імплантованим БЕН, які здійснюють представництво КНЕДП – АЦСК МВС, з використанням програмних засобів робочої станції для оформлення та видачі документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус.

У разі генерації чергових пар ключових даних на БЕН, імплантований у паспорт громадянина України, фізична особа, на ім'я якої оформлено цей паспорт, самостійно із використанням засобів КЕП, наданих КНЕДП – АЦСК МВС генерує ключові дані. КНЕДП – АЦСК МВС та суб'єкти, що здійснюють представництво КНЕДП – АЦСК МВС, можуть надавати допомогу в генерації на БЕН чергових пар ключових даних в офісах у разі їх особистого відвідування фізичними особами, на ім'я яких оформлено паспорт громадянина України з імплантованим БЕН.

Подання та оброблення запитів на сертифікацію, поданих до КНЕДП – АЦСК МВС, здійснюється відповідно до розділу 4 цієї Політики сертифіката.

### 6.1.2. Доставка особистого ключа користувачу

Отримання користувачем особистого ключа у володіння в результаті надання КНЕДП – АЦСК МВС кваліфікованої електронної довірчої послуги здійснюється за таких умов:

- отримання та використання особистого ключа на правах повного володіння засобом КЕП, у тому числі, носієм особистого ключа;

- отримання та використання особистого ключа на правах повного володіння або доступу на договірних засадах до частини ресурсу засобу КЕП, який реалізує зберігання множини особистих ключів кваліфікованого електронного підпису чи печатки (наприклад, мережний криптомодуль).

Фактичне отримання користувачем особистого ключа відбувається у момент генерації такого ключа особисто.

Відповідні Положення сертифікаційних практик містять додаткову інформацію.

### 6.1.3. Доставка відкритого ключа користувачу

Відкритий ключ надається для формування кваліфікованого сертифіката у складі запиту на формування кваліфікованого сертифіката, який являє собою файл формату PKCS#10, що містить відкритий ключ користувача і додаткову інформацію для формування кваліфікованого сертифіката.

Запит формату PKCS#10 формується під час генерації особистого та відкритого ключів засобами кваліфікованого електронного підпису чи печатки. Формування запиту передбачає створення удосконаленого електронного підпису за допомогою особистого ключа з однієї пари з відкритим ключем.

### 6.1.4. Доставка відкритого ключа КНЕДП – АЦСК МВС суб'єктам, які йому довіряють

Кваліфіковані сертифікати КНЕДП – АЦСК МВС та ЦЗО, публікуються на веб-сайті КНЕДП – АЦСК МВС.

Контейнер ланцюжків сертифікатів, доступний для завантаження суб'єктами, які довіряють КНЕДП – АЦСК МВС, розміщений на веб-сайті КНЕДП – АЦСК МВС за посиланням: https://ca.mvs.gov.ua/ca-certificates.

Доступ до актуального кваліфікованого сертифіката КНЕДП – АЦСК МВС забезпечено на офіційному веб-сайті ЦЗО за посиланням: https://czo.gov.ua/ca-registry-details?type=0&id=122.

### 6.1.5. Розміри (параметри) ключів

В ІКС КНЕДП – АЦСК МВС використовуються особисті та відповідні їм відкриті ключі з параметрами, що відповідають алгоритму електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт згідно із ДСТУ 4145-2002.

### 6.1.6. Генерація параметрів відкритого ключа

Під час генерації відкритого ключа використовується апаратна генерація ключів генератор випадкових чисел (ГВЧ), що включає в себе статистичну перевірку виходу генератора. Статистична перевірка випадкових бітових послідовностей з апаратного ГВЧ здійснюється відповідно до Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами. Ключі генеруються та зберігаються у засобі КЕП.

### 6.1.7. Основні цілі використання особистого ключа КНЕДП – АЦСК МВС

Особисті ключі КНЕДП – АЦСК МВС забезпечують функціонування ІКС КНЕДП – АЦСК МВС.

КНЕДП – АЦСК МВС визначає практику використання ключів КНЕДП – АЦСК МВС для підпису сертифікатів користувачів, сертифікатів серверів OCSP, CMP КНЕДП – АЦСК МВС, списку відкликаних сертифікатів (CRL).

## 6.2. Захист особистого ключа та інженерний контроль криптографічного модуля

### 6.2.1. Стандарти та елементи керування криптографічним модулем

Для зберігання особистих ключів користувачів КНЕДП – АЦСК МВС використовує засоби КЕП, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів.

Для зберігання особистих ключів КНЕДП – АЦСК МВС та серверів ІКС КНЕДП – АЦСК МВС використовуються мережні криптомодулі, що виконані у вигляді окремих апаратних

пристроїв. Криптомодулі повинні мати документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів.

### 6.2.2. Особистий ключ (n з m) керування кількома особами

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 6.2.3. Управління особистим ключем підписувача

КНЕДП – АЦСК МВС забезпечує зберігання та захист особистих ключів користувачів, згенерованих в мережних криптомодулях Гряда-301 (високопродуктивний пристрій), які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів, які розміщені в приміщенні резервного ПТК КНЕДП – АЦСК МВС, доступ до яких мають тільки відповідальні особи КНЕДП – АЦСК МВС.

### 6.2.4. Резервне копіювання особистого ключа

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 6.2.5. Архівація особистого ключа

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 6.2.6. Відновлення особистого ключа

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 6.2.7. Зберігання особистого ключа

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 6.2.8. Активація особистих ключів

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 6.2.9. Деактивація особистих ключів

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 6.2.10. Знищення особистих ключів

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 6.2.11. Можливості мережного криптографічного модуля

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 6.3. Інші аспекти керування парами ключів

#### 6.3.1. Архівація відкритого ключа

Відкриті ключі, на основі яких сформовано кваліфіковані сертифікати зберігаються в базі даних КНЕДП – АЦСК МВС постійно.

#### 6.3.2. Строки дії сертифіката та строки використання пари ключів

Строки дії особистих ключів КНЕДП – АЦСК МВС відповідають строкам чинності кваліфікованих сертифікатів відповідних їм відкритих ключів і становлять:

- для особистих ключів КНЕДП – АЦСК МВС та його серверів (OCSP, CMP, TSP) – не більше 5 років;

- для особистих ключів адміністраторів та користувачів - не більше 2 років.

### 6.4. Дані активації

#### 6.4.1. Створення та встановлення даних активації

Відповідно до пункту 3.2 цієї Політики сертифіката.

#### 6.4.2. Захист даних активації

Всі особисті ключі, які зберігаються у засобах КЕП, захищаються паролями шляхом вироблення імітовставки та шифрування. Паролі повинні відповідати наступним вимогам:

– алфавіт символів пароля – англійські букви “a” – “z”, “A” – “Z”, цифри “0” – “9” та символи “-”, “+” (потужність алфавіту – $2^6$, 6 біт/символ);

– довжина пароля – мінімальна 8, максимальна 42 символи (48-252 біт, потужність системи паролювання $2^{48}$-$2^{252}$);

– обмеження до використання символів в паролі – не допускається введення більш ніж 2-ох символів, що розташовані поруч на розкладці клавіатури, не допускається введення більш ніж 2-ох однакових символів на всій довжині пароля.

#### 6.4.3. Інші аспекти даних активації

Відсутні.

### 6.5. Контроль комп'ютерної безпеки

#### 6.5.1. Спеціальні технічні вимоги до комп’ютерної безпеки

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 6.5.2. Рейтинг комп'ютерної безпеки

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

## 6.6. Контроль безпеки життєвого циклу

### 6.6.1. Контроль розробки системи

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 6.6.2. Засоби керування безпекою

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

### 6.6.3. Контроль безпеки протягом життєвого циклу

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

## 6.7. Контроль безпеки мережі

Цей розділ не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами.

## 6.8. Електронні позначки часу

### 6.8.1. Формування кваліфікованої електронної позначки часу

Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження кваліфікованої електронної позначки часу надається користувачам при створенні КЕП.

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

Кваліфікована електронна позначка часу повинна відповідати таким вимогам:

- пов'язувати дату і час з електронними даними в такий спосіб, що обґрунтовано виключає можливість зміни електронних даних, яка не може бути виявлена;

- базуватися на джерелі точного часу, синхронізованому із Всесвітнім координованим часом (UTC) з точністю до секунди;

- до кваліфікованої електронної позначки часу додається створений для неї удосконалений електронний підпис чи удосконалена електронна печатка КНЕДП – АЦСК МВС або може застосовувати інший метод, рівнозначний додаванню до кваліфікованої електронної позначки часу удосконаленого електронного підпису чи удосконаленої електронної печатки, за умови що він забезпечує рівнозначний рівень безпеки кваліфікованої електронної позначки часу та відповідає вимогам Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

### 6.8.2. Перевірка кваліфікованої електронної позначки часу

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 КНЕДП – АЦСК МВС;
2) перевіряє КЕП, накладений на кваліфіковану електронну позначку часу за допомогою чинного (на момент формування кваліфікованої електронної позначки часу) кваліфікованого сертифіката КНЕДП – АЦСК МВС;
3) перевіряє відповідність кваліфікованої електронної позначки часу та електронних даних, до яких вона додана.

### 6.8.3. Недійсність кваліфікованої електронної позначки часу

Кваліфікована електронна позначка часу вважається недійсною у разі:

- недотримання вимоги щодо точності часу в програмно-технічному комплексі КНЕДП – АЦСК МВС;

- використання скасованого або блокованого сертифіката КНЕДП – АЦСК МВС на

момент формування кваліфікованої електронної позначки часу.

Правильність реалізації криптографічних алгоритмів для створення кваліфікованої електронної позначки часу та точність часу в засобі кваліфікованого електронного підпису чи печатки (QSCD) забезпечує протокол фіксування часу.

### 6.8.4. Отримання кваліфікованої електронної позначки часу КНЕДП – АЦСК МВС

КНЕДП – АЦСК МВС отримує кваліфіковану електронну довірчу послугу з формування, перевірки та підтвердження кваліфікованої електронної позначки часу від ЦЗО.

Механізм синхронізації часу із Всесвітнім координованим часом (UTC) в програмно-технічному комплексі КНЕДП – АЦСК МВС та склад технічного обладнання, що застосовується у процесі синхронізації часу (його загальний опис) встановлюється Порядком синхронізації часу із Всесвітнім координованим часом (UTC).

Порядок синхронізації часу із Всесвітнім координованим часом (UTC) розробляється КНЕДП – АЦСК МВС та погоджується з ЦЗО.

## 7. ПРОФІЛІ СЕРТИФІКАТІВ, СПИСКІВ ВІДКЛИКАНИХ СЕРТИФІКАТІВ (CRL) ТА ПРОТОКОЛУ ВИЗНАЧЕННЯ СТАТУСУ СЕРТИФІКАТА (OCSP)

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.6 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

### 7.1. Профілі сертифікатів

Кваліфіковані сертифікати, що формуються КНЕДП – АЦСК МВС повинні відповідати вимогам таких стандартів:

- ДСТУ ISO/IEC 9594-8:2021 (ISO/IEC 9594-8:2020, IDT) «Інформаційні технології. Взаємозв’язок відкритих систем. Частина 8. Каталог. Структура сертифікатів відкритих ключів та атрибутів» (далі - ISO/IEC 9594-8:2020)$

- ДСТУ ETSI EN 319 412-1:2021 (ETSI EN 319 412-1 V1.4.4 (2021-05), IDT) «Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та типові структури даних» (далі - ДСТУ ETSI EN 319 412-1:2021);

- ДСТУ ETSI EN 319 412-2:2021 (ETSI EN 319 412-2 V2.2.1 (2020-07), IDT) «Електронні підписи та інфраструктури. (ESI). Профілі сертифікатів. Частина 2. Профілі сертифікатів, виданих фізичним особам» (далі - ДСТУ ETSI EN 319 412-2:2021);

- ДСТУ ETSI EN 319 412-3:2021 (ETSI EN 319 412-3 V1.2.1 (2020-07), IDT) «Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 3. Профілі сертифікатів, виданих юридичним особам»;

- ДСТУ ETSI EN 319 412-4:2022 (ETSI EN 319 412-4 V1.2.1 (2021-11), IDT) «Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 4. Профіль сертифіката для сертифікатів веб-сайтів»;

- ДСТУ ETSI EN 319 412-5:2022 (ETSI EN 319 412-5 V2.3.1 (2020-04), IDT) «Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 5. Розширення сертифікатів QCStatements»;

- ДСТУ ETSI TS 119 312 (ETSI;TS 119 312, IDT) «Електронні підписи та інфраструктури (ESI). Криптографічні набори»;

- ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», (далі - ДСТУ 4145-2002);

Поля та формат інформації, що міститься в кваліфікованому сертифікаті:

| **Найменування** | **Значення** |
|---|---|
| Версія | Версія 3 (версія 3) стандарт X.509 |
| Серійний Номер | Номер сертифіката<br>Значення цього поля є унікальним |
| Алгоритм підпису | Криптографічний алгоритм<br>Визначає алгоритм, якийвикористовується для підпису кваліфікованого сертифіката |
| Емітент | Назва КНЕДП, що формує кваліфікований сертифікат |
| Дійсний від | Дата початку дії кваліфікованого сертифіката (відповідно до стандарту RFC 5280) |
| Дійсний до | Дата закінчення строку дії кваліфікованого сертифіката (відповідно до стандарту RFC 5280) |
| Тема | Інформація про отримувача кваліфікованого сертифіката (відповідно до стандарту RFC 5280)<br>Детальніше див. п. 3.1.1 |
| Відкритий ключ | Відкритий ключ, що відповідає особистому ключу кваліфікованого сертифіката (відповідно до стандарту RFC 5280) |
| Підпис | Кваліфікований електронний підпис КНЕДП – АЦСК МВС, що надає послугу створення, перевірки та підтвердження КЕП<br>Згенерований та закодований відповідно до стандарту RFC 5280. |

### 7.2. Профілі списку відкликаних сертифікатів (CRL)

Списки відкликаних сертифікатів (CRL), що формуються КНЕДП – АЦСК МВС повинні відповідати вимогам таких стандартів:

- ДСТУ ISO/IEC 9594-8:2021 (ISO/IEC 9594-8:2020, IDT) “Інформаційні технології. Взаємозв'язок відкритих систем. Частина 8. Каталог. Структура сертифікатів відкритих ключів та атрибутів” (далі - ISO/IEC 9594-8:2020);

- Формат інформації в CRL, що публікується КНЕДП – АЦСК МВС, відповідає стандарту ITU-TX.509 та регламенту RFC 5280. CRL повинен мати щонайменше такі поля:

| **Найменування** | **Значення** |
|---|---|
| Версія | Версія CRL (version 2). |
| Емітент | Назва КНЕДП – АЦСК МВС, що формує CRL |
| Дата набрання чинності | Поточна дата випуску (оновлення) CRL |
| Наступне оновлення | Дата наступного оновлення CRL |
| Скасовані сертифікати | У цьому полі міститься інформація про скасовані кваліфіковані сертифікати, зокрема:<br>- Серійний номер (серійний номер скасованого кваліфікованого сертифіката);<br>- дата скасування (час, коли кваліфікований сертифікат було скасовано);<br>- запис про скасування (розширена інформація скасованого кваліфікованого сертифіката (необов'язкове поле) |
| Алгоритм підпису | Алгоритм, що використовується для підписання CRL |
| Алгоритм гешування підпису | Алгоритм гешування |
| Підпис | Значення електронного підпису від КНЕДП – АЦСК МВС |
| Розширення CRL | Інша розширена інформація (необов'язкове поле) |

### 7.3. Профілі протоколу визначення статусу сертифіката (OCSP)

Розповсюдження інформації про статус кваліфікованих сертифікатів користувачів здійснюється шляхом створення можливості перевірки статусу кваліфікованого сертифіката користувача в режимі реального часу через електронні комунікаційні мережі загального користування із використанням протоколу OCSP.

Посилання на сервіс перевірки статусу кваліфікованого сертифіката користувача в режимі реального часу вносяться до кваліфікованих сертифікатів користувачів.

Процедура інтерактивного визначення статусу сертифіката та формати даних повинні відповідати вимогам таких стандартів:

- ISO/IEC 8825-1:2002 “Information technology - ASN.1 Encoding Rules - Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER);

- RFC 2560 “Internet X.509 Public Key Infrastructure Online Certificate Status;

- Protocol - OCSP”.

## 8. АУДИТ ВІДПОВІДНОСТІ ТА ІНШІ ОЦІНКИ

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.7 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

### 8.1. Частота або обставини оцінювання

Не допускається надання кваліфікованих електронних довірчих послуг без чинних документів, визначених законодавством, що підтверджують відповідність ІКС КНЕДП – АЦСК МВС та засобів захисту інформації у її складі вимогам нормативно-правових актів у сфері технічного та криптографічного захисту інформації, або документів про відповідність, за результатами проходження процедури оцінки відповідності, у сфері електронних довірчих послуг.

КНЕДП – АЦСК МВС знаходиться під наглядом КО, функції якого виконує Адміністрація Державної служби спеціального зв'язку та захисту інформації України.

КО у випадках, визначених законом, може:

1) здійснити позапланову перевірку щодо дотриманням КНЕДП вимог законодавства у сфері електронних довірчих послуг:

- за його заявою;

- у разі виявлення та підтвердження наявності недостовірних відомостей у поданих ним документах;

- після отримання інформації чи повідомлення про порушення вимог законодавства у сфері електронних довірчих послуг від ЦЗО, суду, користувачів або третіх осіб;

- за обґрунтованим рішенням КО.

КО не здійснює планові заходи контролю.

2) подати запит до ООВ про надання аудиторського звіту щодо проведення процедури оцінки відповідності КНЕДП за його рахунок для підтвердження того, що він та електронні довірчі послуги, які він надає, відповідають вимогам у сфері електронних довірчих послуг.

Про результати оцінки відповідності КНЕДП повідомляє КО шляхом надання копії документа про відповідність не пізніше трьох робочих днів з дня його отримання.

Оцінку відповідності проводить ООВ, як зазначено в розділі 8.2 цієї Політики сертифіката.

КНЕДП – АЦСК МВС проходить оцінку відповідності згідно з вимогами:

- ДСТУ ETSI EN 319 401;
- ДСТУ ETSI EN 319 411-1;

- ДСТУ ETSI EN 319 411-2.

Сертифікат підтвердження відповідності ІКС КНЕДП – АЦСК МВС, отриманий за результатами проходження процедури сертифікації, діє протягом визначеного в сертифікаті строку дії.

### 8.2. Особа/кваліфікація оцінювача

#### 8.2.1. Вимоги до кваліфікації контролюючого органу (КО)

Функції КО виконує Державна служба спеціального зв'язку та захисту інформації України.

Виїзний позаплановий захід державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг (далі - перевірка) здійснюється посадовими особами КО відповідно до їх функціональних обов'язків за місцезнаходженням КНЕДП – АЦСК МВС.

Перевірка здійснюється відповідно до рішення КО.

Рішення щодо проведення перевірки повинно містити:

1) найменування Адміністрації Держспецзв'язку;
2) найменування КНЕДП,
3) місцезнаходження КНЕДП;
4) підставу для проведення перевірки;
5) предмет перевірки;
6) дати початку та закінчення перевірки;
7) посадовий та персональний склад комісії з перевірки.

#### 8.2.2. Вимоги до кваліфікації органу з оцінки відповідності (ООВ)

ООВ - це підприємство, установа, організація чи її структурний підрозділ, що провадить діяльність з оцінки відповідності у сфері електронних довірчих послуг та акредитований національним органом з акредитації або іноземним органом з акредитації, який є підписантом багатосторонньої угоди про визнання Міжнародного форуму з акредитації та/або Європейської кооперації з акредитації (EA MLA).

ООВ повинен мати відповідну компетенцію для здійснення оцінки відповідності щодо підтвердження відповідності вимогам до КНЕДП та послуг, що ними надаються.

ООВ повинен дотримуватися положень, визначених у стандарті ДСТУ ETSI EN 319 403-1 (ETSI EN 319 403-1, IDT) «Електронні підписи та інфраструктури (ESI). Оцінювання відповідності постачальників довірчих послуг. Частина 1. Вимоги до органів оцінювання відповідності, які оцінюють постачальників довірчих послуг», затвердженому наказом державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 16 грудня 2021 р. № 512.

#### 8.2.3. Вимоги до кваліфікації організації, що проводить експертизу КСЗІ

Державна експертиза КСЗІ в ІКС КНЕДП – АЦСК МВС проводиться згідно з Положенням про державну експертизу в сфері технічного захисту інформації, затвердженим наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087, та НД ТЗІ 2.6-001-11 «Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах».

Організація, що провела експертизу КСЗІ в ІКС КНЕДП – АЦСК МВС (далі – Організатор експертизи), призначена Адміністрацією Держспецзв'язку після розгляду заяви Міністерства внутрішніх справ України на проведення державної експертизи КСЗІ в ІКС КНЕДП – АЦСК МВС.

Організатор експертизи виконав роботу з експертизи КСЗІ в ІКС КНЕДП – АЦСК МВС відповідно до вимог ліцензії на провадження господарської діяльності з надання послуг в галузі технічного захисту інформації.

### 8.3. Відносини експерта з об'єктом оцінки

#### 8.3.1. Відносини посадових осіб контролюючого органу (КО) з об'єктом оцінки

Відповідно до частини шостої статті 4 Закону України "Про основні засади державного нагляду (контролю) у сфері господарської діяльності" посадовій особі органу державного нагляду (контролю) забороняється здійснювати державний нагляд (контроль) щодо суб'єктів господарювання, з якими (або із службовими особами яких) посадова особа перебуває в родинних стосунках, або в разі виникнення у неї конфлікту інтересів згідно із законодавством у сфері запобігання і протидії корупції.

Члени комісії з перевірки зобов'язані:

- об'єктивно та неупереджено проводити перевірку;
- дотримуватися вимог законодавства у сферах електронної ідентифікації, електронних довірчих послуг, захисту інформації та захисту персональних даних;
- сумлінно, вчасно та якісно виконувати свої службові обов'язки та доручення голови комісії з перевірки;
- дотримуватися ділової етики у взаємовідносинах з керівником та персоналом КНЕДП – АЦСК МВС;
- ознайомлювати керівника КНЕДП – АЦСК МВС чи уповноваженого ним представника з результатами перевірки;
- надавати КНЕДП – АЦСК МВС консультаційну допомогу з питань проведення перевірки;
- не розголошувати інформацію з обмеженим доступом, яка стала їм відома у зв'язку з виконанням службових обов'язків.

#### 8.3.2. Відносини експертів (аудиторів), що проводять оцінку відповідності, з об'єктом оцінки

Експерти (аудитори), що проводять оцінку відповідності, повинні бути незалежними та не мати спільних ділових інтересів та жодного ділового зв'язку з КНЕДП – АЦСК МВС.

#### 8.3.3. Відносини експертів, що проводять експертизу з об'єктом експертизи КСЗІ

Виконавці експертних робіт з технічного захисту інформації – це фізичні особи, які на постійній або професійній основі здійснюють діяльність, пов'язану з наданням експертних послуг (далі – Експерти).

Під час проведення експертизи кожний Експерт виконує експертні роботи тільки за дорученням Організатора експертизи та відповідно до визначеної методики. Кількість і персональний склад Експертів, які залучаються до виконання експертних робіт, визначає Організатор експертизи.

До проведення експертизи КСЗІ в ІКС КНЕДП – АЦСК МВС не можуть залучатися Експерти, які виконували роботи зі створення КСЗІ в ІКС КНЕДП – АЦСК МВС (у тому числі надавали консультаційні послуги щодо виконання окремих етапів робіт та вибору певних проектних рішень).

### 8.4. Теми, охоплені оцінюванням

#### 8.4.1. Питання, що підлягають перевірці під час державного контролю

Предметом перевірки, що проводиться КО є стан дотримання вимог законодавства у сфері електронних довірчих послуг, у тому числі цієї Політики сертифіката та відповідних Положень сертифікаційних практик за такими питаннями:

- загальні вимоги;
- забезпечення безпеки інформаційних ресурсів;
- кадрові ресурси;
- експлуатація засобів кваліфікованого електронного підпису чи печатки;
- вимоги до надання електронних довірчих послуг;
- політика сертифіката;
- положення сертифікаційних практик;
- надання кваліфікованої електронної довірчої послуги із створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток;
- забезпечення безпеки фізичного доступу до приміщень.

#### 8.4.2. Питання, що підлягають перевірці під час оцінки відповідності

Предметом оцінки відповідності, що проводиться ООВ, є стан дотримання вимог ДСТУ ETSI EN 319 401.

#### 8.4.3. Питання, що підлягають перевірці під час експертизи КСЗІ

Питання, що підлягають перевірці під час експертизи КСЗІ в ІКС КНЕДП, визначаються розділом 7 «Опис порядку проведення робіт з експертизи комплексних систем захисту інформації» НД ТЗІ 2.6-001-11 «Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах».

### 8.5. Дії, вжиті внаслідок порушення

#### 8.5.1. Дії, що вживаються внаслідок порушення, виявленого за результатами державного контролю

Посадові особи КО під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг мають право:

- здійснювати виїзні та невиїзні заходи державного нагляду (контролю) за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг;

- у разі виявлення порушення вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг видавати обов'язкові для виконання приписи про усунення порушень і визначати строк усунення виявлених порушень;

- накладати на винних осіб адміністративні стягнення за порушення вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги» та інших нормативно-правових актів, прийнятих відповідно до цього Закону;
- звертатися до суду щодо застосування заходів реагування;

- виконувати інші повноваження, визначені законом.

За результатами проведення перевірок КО вживає таких заходів реагування:

1) вимагає від КНЕДП – АЦСК МВС усунення порушень вимог законодавства у сфері електронних довірчих послуг у встановлений приписом строк;

2) приймає рішення про блокування кваліфікованого сертифіката КНЕДП – АЦСК МВС, якщо під час перевірки виникла підозра компрометації особистого ключа;

3) приймає рішення про скасування кваліфікованого сертифіката КНЕДП – АЦСК МВС, якщо під час перевірки виявлено факт компрометації особистого ключа.

Рішення про блокування або скасування кваліфікованого сертифіката КНЕДП – АЦСК МВС КО надсилає в день його прийняття до ЦЗО;

4) надсилає до ЦЗО подання про відкликання статусу КНЕДП або послуги, яку надає КНЕДП – АЦСК МВС, у Довірчому списку в разі:

- надання КЕД послуг КНЕДП – АЦСК МВС без чинних документів, визначених законодавством,

- відповідність комплексної системи захисту інформації інформаційно-комунікаційної системи кваліфікованого надавача електронних довірчих послуг та засобів захисту інформації у її складі вимогам нормативно-правових актів у сфері технічного та криптографічного захисту інформації, або документів про відповідність за результатами процедури оцінки відповідності у сфері електронних довірчих послуг;

- непроходження додаткової державної експертизи комплексної системи захисту інформації або процедури оцінки відповідності інформаційно-комунікаційної системи кваліфікованого надавача електронних довірчих послуг у разі модернізації апаратного, апаратно-програмного пристрою чи програмного забезпечення, що входять до складу програмно-технічного комплексу, яка не передбачена проектною чи експлуатаційною документацією до КСЗІ в ІКС КНЕДП – АЦСК МВС;

- надання кваліфікованих електронних довірчих послуг за відсутності у КНЕДП – АЦСК МВС поточного рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) з необхідним обсягом коштів або чинного договору страхування цивільно-правової відповідальності з необхідним розміром страхової суми, що встановлені Законом України "Про електронну ідентифікацію та електронні довірчі послуги", для забезпечення відшкодування збитків, які можуть бути завдані користувачам електронних довірчих послуг або третім особам внаслідок неналежного виконання КНЕДП – АЦСК МВС своїх зобов'язань;

- порушення вимог до умов експлуатації комплексної системи захисту інформації інформаційно-комунікаційної системи в ІКС послуг КНЕДП – АЦСК МВС;

- надання кваліфікованих електронних довірчих послуг КНЕДП – АЦСК МВС без чинних документів, визначених законодавством, що підтверджують його право власності та/або право користування засобами кваліфікованого електронного підпису чи печатки, які використовуються для надання кваліфікованих електронних довірчих послуг;

- встановлення факту надання недостовірних відомостей, наведених у документах, поданих КНЕДП – АЦСК МВС для внесення відомостей про нього до Довірчого списку;

- неусунення виявлених під час перевірки порушень у встановлений приписом строк;

- блокування або скасування кваліфікованого сертифіката КНЕДП – АЦСК МВС.

### 8.5.2. Дії, що вживаються внаслідок порушення, виявленого за результатами оцінки відповідності

За результатами проведення процедури оцінки відповідності у сфері електронних довірчих послуг ООВ приймається одне з таких рішень:

- про відповідність об'єкта оцінки відповідності у повному обсязі вимогам у сфері електронних довірчих послуг;

- про невідповідність об'єкта оцінки відповідності вимогам у сфері електронних довірчих послуг.

У разі прийняття рішення про невідповідність об'єкта оцінки відповідності вимогам у сфері електронних довірчих послуг ООВ видає замовнику процедури оцінки відповідності аудиторський звіт з висновками про невідповідність з переліком недоліків.

Результати оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг аналізуються КО. У разі негативних результатів оцінки відповідності та/або наданих органом з оцінки відповідності рекомендацій контролюючий орган може своїм рішенням призначити додаткову оцінку відповідності після усунення всіх недоліків, зазначених в аудиторському звіті.

КО надсилає до ЦЗО подання про відкликання статусу КНЕДП або послуги, яку надає КНЕДП, у Довірчому списку в разі надання КЕД послуг КНЕДП без чинних документів, визначених законодавством, що підтверджують відповідність комплексної системи захисту інформації ІКС КНЕДП – АЦСК МВС та засобів захисту інформації у її складі вимогам нормативно-правових актів у сфері технічного та криптографічного захисту інформації, або документів про відповідність за результатами процедури оцінки відповідності у сфері електронних довірчих послуг.

### 8.5.3. Дії, що вживаються внаслідок порушення, виявленого під час експертизи КСЗІ

У разі виявлення невідповідності КСЗІ в ІКС КНЕДП – АЦСК МВС вимогам нормативних документів з технічного захисту інформації Організатор експертизи може запропонувати Міністерству внутрішніх справ України виконати доопрацювання.

Строк доопрацювання КСЗІ в ІКС КНЕДП – АЦСК МВС визначається спільним протоколом або додатковою угодою до договору між Міністерством внутрішніх справ України та Організатором експертизи. Відомості щодо всіх доопрацювань, а також результати додаткових експертних робіт оформлюються окремими протоколами.

## 8.6. Повідомлення результатів

### 8.6.1. Оформлення результатів державного контролю

Результати проведення перевірки КНЕДП – АЦСК МВС оформлюються комісією з перевірки шляхом складення акта перевірки, форма якого затверджується КО.

Акт перевірки має містити такі відомості:

- найменування КО;

- персональний та посадовий склад комісії з перевірки;

- прізвище та ініціали керівника КНЕДП – АЦСК МВС;

- реквізити посвідчення на проведення перевірки;

- дати початку і закінчення перевірки;

- адреса приміщень КНЕДП – АЦСК МВС, в яких проводилася перевірка;

- результати попередньої перевірки;

- інформація про результати останньої оцінки відповідності у сфері електронних довірчих послуг, що передує перевірці;

- назва та короткий зміст документів, наданих під час перевірки;

- якісні та кількісні показники, встановлені під час перевірки, що характеризують діяльність КНЕДП – АЦСК МВС, пов'язану з наданням електронних довірчих послуг;

- виявлені під час перевірки порушення і недоліки (за наявності) та пояснення КНЕДП – АЦСК МВС про причини невиконання встановлених законодавством вимог (за наявності);

- висновки за результатами перевірки;

- факти протидії проведенню перевірки (за наявності);

- рекомендації щодо усунення виявлених порушень (у разі наявності);

- дата складення акта перевірки;

- підписи голови та членів комісії з перевірки;

- підпис керівника КНЕДП – АЦСК МВС чи уповноваженого ним представника, що підтверджує факт ознайомлення з актом перевірки.

Акт перевірки складається у двох примірниках та підписується не пізніше останнього дня її проведення головою та всіма членами комісії з перевірки і керівником КНЕДП – АЦСК МВС чи уповноваженим ним представником.

Член комісії з перевірки, який не погоджується з висновками комісії з перевірки, зазначеними в акті перевірки, зобов'язаний підписати його та письмово викласти свою окрему думку, що додається до акта перевірки. При цьому перед підписом акта перевірки зазначається "З окремою думкою, що додається".

Якщо керівник КНЕДП – АЦСК МВС чи уповноважений ним представник має зауваження щодо фактів та висновків, викладених в акті перевірки, перед підписом зазначається «Із зауваженнями, що додаються».

Зауваження до акта перевірки оформлюються окремим документом та підписуються керівником КНЕДП – АЦСК МВС чи уповноваженим ним представником.

Зауваження до акта перевірки та окрема думка члена комісії з перевірки є невід'ємними частинами акта перевірки.

Якщо керівник КНЕДП – АЦСК МВС чи уповноважений ним представник відмовився від ознайомлення з актом перевірки або від його підписання після ознайомлення з ним, голова комісії з перевірки перед місцем для підпису керівника КНЕДП – АЦСК МВС чи уповноваженого ним представника робить відповідне зазначення, яке засвідчується підписами голови та одного з членів комісії з перевірки.

### 8.6.2. Припис про усунення порушень, виявлених під час державного контролю

Посадові особи КО під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг мають право у разі виявлення порушення вимог законодавства у сфері електронних довірчих послуг видавати

обов'язкові для виконання приписи про усунення порушень і визначати строк усунення виявлених порушень.

Припис про усунення порушень складається комісією з перевірки у двох примірниках протягом п'яти робочих днів після завершення перевірки. Один примірник припису не пізніше п'яти робочих днів з дня складення акта перевірки надається КНЕДП – АЦСК МВС, а другий примірник з підписом керівника КНЕДП – АЦСК МВС чи уповноваженого ним представника щодо погоджених строків усунення порушень вимог законодавства у сфері електронних довірчих послуг залишається у КО.

Форма припису про усунення порушень затверджується КО.

Припис про усунення порушень підписується головою та членами комісії з перевірки, які їх проводили.

У разі якщо керівник КНЕДП – АЦСК МВС чи уповноважений ним представник відмовився від отримання припису про усунення порушень, такий припис надсилається рекомендованим листом, а на копії припису, що залишається у КО, проставляються відповідний вихідний номер і дата надсилання.

Керівник КНЕДП – АЦСК МВС повинен вжити заходів до усунення недоліків та порушень, зазначених у приписі про усунення порушень, протягом визначеного у приписі строку.

КНЕДП – АЦСК МВС зобов'язаний у визначений у приписі про усунення порушень строк письмово подати до КО інформацію про усунення порушень разом з підтвердними документами.

### 8.6.3. Оформлення результатів оцінки відповідності

Документ про відповідність повинен містити такі відомості:

- найменування ООВ;

- інформацію про акредитацію ООВ (дата та номер атестата про акредитацію);

- прізвище, ім'я, по батькові (у разі наявності) осіб, що проводили процедуру оцінки відповідності;

- період проведення процедури оцінки відповідності;

- реквізити КНЕДП – АЦСК МВС (найменування, ідентифікаційні дані та контактна інформація);

- сфера оцінки відповідності;

- перелік кваліфікованих електронних довірчих послуг, які має намір надавати КНЕДП – АЦСК МВС;

- найменування ІКС;

- найменування засобів кваліфікованого електронного підпису, які використовуються під час надання кваліфікованих електронних довірчих послуг;

- перелік вимог у сфері електронних довірчих послуг, національних стандартів та/або технічних специфікацій, щодо відповідності яким проводилася процедура оцінка відповідності;

- висновок щодо відповідності вимогам у сфері електронних довірчих послуг;

- строк дії документа про відповідність.

Про результати проведення процедури планової та повторної (позапланової) оцінки відповідності у сфері електронних довірчих послуг КНЕДП – АЦСК МВС повинен повідомити КО шляхом надання копій документів про відповідність (за наявності) та аудиторських звітів не пізніше трьох робочих днів з дня їх отримання.

ООВ надає публічний доступ до актуальної інформації про результати оцінки відповідності у сфері електронних довірчих послуг.

#### 8.6.4. Оформлення результатів експертизи КСЗІ

За результатами проведених робіт Організатором експертизи складено на КСЗІ в ІКС КНЕДП – АЦСК МВС експертний висновок згідно з додатком 6 до Положення про державну експертизу у сфері технічного захисту інформації, затвердженим наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087, та згідно з позитивними результатами експертної оцінки – атестат відповідності згідно з додатком 7 до Положення про державну експертизу у сфері технічного захисту інформації, затвердженим наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93, зареєстрованим в Міністерстві юстиції України 16.07.2007 за № 820/14087.

Зазначені документи засвідчені Організатором експертизи і разом з програмою, методикою та протоколами виконання робіт подано до Адміністрації Держспецзв'язку (в тому числі в електронному вигляді у форматі.pdf).

### 8.7. Самоперевірки

Протягом періоду формування сертифікатів, КНЕДП – АЦСК МВС контролює дотримання цієї Політики сертифіката та відповідних Положень сертифікаційних практик, суворо контролюючи якість своїх послуг, час від часу виконуючи самоперевірки, виданих сертифікатів.

КНЕДП – АЦСК МВС проводить регулярні внутрішні аудити, щоб оцінювати дотримання вимог законодавства, внутрішньої політики та вимог цієї Політики сертифіката та відповідних Положень сертифікаційних практик щонайменше раз на рік.

## 9. ІНШІ КОМЕРЦІЙНІ ТА ЮРИДИЧНІ ПИТАННЯ

До об'єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.8 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

### 9.1. Плата за кваліфіковані електронні послуги, що надаються КНЕДП – АЦСК МВС

#### 9.1.1. Плата за видачу або поновлення сертифіката

Плата за видачу або поновлення сертифіката відсутня.

#### 9.1.2. Плата за доступ до сертифіката

Плата за доступ до кваліфікованого сертифіката відсутня.

#### 9.1.3. Плата за блокування/скасування або доступ до інформації про статус сертифіката

Плата за блокування/скасування кваліфікованого сертифіката або доступ до інформації про статус кваліфікованого сертифіката відсутня.

#### 9.1.4. Плата за інші послуги

Плата за інші послуги відсутня.

#### 9.1.5. Політика відшкодування

Відшкодування здійснюється у випадку, передбаченому розділом 9.2 цієї Політики сертифіката.

### 9.2. Фінансова відповідальність

Діяльність КНЕДП – АЦСК МВС відповідає вимогам частини п'ятої статті 16 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» щодо надання КЕД послуг за умови внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) для забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам внаслідок неналежного виконання КНЕДП – АЦСК МВС, ВПР КНЕДП – АЦСК МВС своїх зобов'язань, або страхування відповідальності для забезпечення відшкодування такої шкоди.

Розмір внеску на поточному рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми не може становити менше 1 тисячі розмірів мінімальної заробітної плати.

### 9.3. Конфіденційність ділової інформації

#### 9.3.1. Обсяг конфіденційної інформації

В процесі надання послуг, КНЕДП – АЦСК МВС обробляє конфіденційну інформацію, яка не оприлюднюється для загального ознайомлення. Захист конфіденційної інформації здійснюється відповідно до чинного законодавства.

#### 9.3.2. Інформація, що не належить до конфіденційної

Інформація та документація, яка є доступною для загального ознайомлення, публікується на веб-сайті КНЕДП – АЦСК МВС та не належить до конфіденційної інформації.

#### 9.3.3. Відповідальність за захист конфіденційної інформації

КНЕДП – АЦСК МВС здійснює захист конфіденційної інформації та несе відповідальність згідно з вимогами чинного законодавства.

### 9.4. Конфіденційність персональної даних

#### 9.4.1. Концепція захисту персональних даних

КНЕДП – АЦСК МВС у процесі надання КЕД послуг здійснює: захист персональних даних користувачів відповідно до вимог Закону України «Про захист персональних даних»:

- захист персональних даних користувачів відповідно до вимог Закону України «Про захист персональних даних»;

- інформування КО та, в разі необхідності, органу з питань захисту персональних даних про порушення конфіденційності та/або цілісності інформації, що впливають на надання кваліфікованих електронних довірчих послуг або стосуються персональних даних

користувачів, без необґрунтованої затримки, не пізніше ніж протягом 24 годин з моменту, коли йому стало відомо про таке порушення;

- інформування користувачів про порушення конфіденційності та/або цілісності інформації, що впливають на надання їм електронних довірчих послуг або стосуються їхніх персональних даних, без необґрунтованої затримки, але не пізніше двох годин з моменту, коли йому стало відомо про таке порушення.

#### 9.4.2. Визначення персональних даних

Поняття «персональні дані» розуміється у значенні, наведеному у статті 2 Закону України «Про захист персональних даних».

#### 9.4.3. Персональні дані, що не вважаються конфіденційними

Персональні дані можуть відноситись до відкритої інформації у випадках, визначених чинним законодавством.

#### 9.4.4. Відповідальність за захист персональних даних

КНЕДП – АЦСК МВС гарантує дотримання вимог законодавства про захист персональних даних та несе відповідальність за порушення конфіденційності та/або цілісності інформації про користувачів під час надання їм КЕД послуг згідно з вимогами чинного законодавства.

Керівник КНЕДП – АЦСК МВС забезпечує створення умов для безперервної особистої освіти та постійне підвищення кваліфікації персоналу КНЕДП – АЦСК МВС у сферах інформаційних технологій, захисту інформації та персональних даних.

#### 9.4.5. Інформація та згода на використання персональних даних

Отриманню КЕД послуг передує надання користувачем згоди на обробку його персональних даних відповідно до Закону України «Про захист персональних даних». КНЕДП – АЦСК МВС надає КЕД послуги відповідно до укладеного договору з користувачем та здійснює обробку персональних даних користувача в межах виконання договору чи для здійснення заходів, що передують укладанню договору на вимогу користувача.

#### 9.4.6. Розкриття персональних даних

КНЕДП – АЦСК МВС надає доступ до персональних даних користувачів лише у випадках, передбачених Законом України «Про захист персональних даних».

Керівник та працівники КНЕДП – АЦСК МВС дотримуються вимог законодавства України у сфері захисту персональних даних та підписують договір про конфіденційність та нерозголошення інформації.

### 9.5. Права інтелектуальної власності

Не застосовується.

### 9.6. Зобов'язання та гарантії

#### 9.6.1. Зобов'язання та гарантії КНЕДП – АЦСК МВС

КНЕДП – АЦСК МВС надає КЕД послуги з дотриманням вимог законодавства у сфері електронних довірчих послуг та цього Регламенту.

### 9.6.2. Зобов'язання та гарантії ВПР КНЕДП – АЦСК МВС

На підставі наказу МВС або договору, укладеного з МВС, реєстрацію користувачів здійснюють ВПР КНЕДП – АЦСК МВС, які виконують свої функції згідно з цією Практикою сертифіката.

До працівників ВПР КНЕДП – АЦСК МВС, на яких покладено обов'язки з реєстрації користувачів, застосовуються такі ж вимоги, як і до адміністраторів реєстрації КНЕДП – АЦСК МВС.

### 9.6.3. Зобов'язання та гарантії користувачів

КНЕДП – АЦСК МВС забезпечує можливість користувачів підписувати та перевіряти підписані файли за допомогою спеціалізованого програмного забезпечення, що розміщені на веб-сайті https://ca.mvs.gov.ua.

Користувачі зобов'язані:

- забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;

- невідкладно повідомляти КНЕДП – АЦСК МВС про підозру або факт компрометації особистого ключа;

- надавати достовірну інформацію, необхідну для отримання КЕД послуг;

- своєчасно надавати КНЕДП – АЦСК МВС інформацію про зміну ідентифікаційних даних, які містить кваліфікований сертифікат;

- не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування кваліфікованого сертифіката.

Користувач гарантує, що:

- для підписання використовує особистий ключ, що відповідає відкритому ключу;

- на момент підписання кваліфікований сертифікат є чинним (не перебуває в статусі блокований або скасований);

- особистий ключ та пароль від нього не скомпрометовані і не використовуються іншими особами;

- вся інформація зазначена в кваліфікованому сертифікаті є коректною;

- кваліфікований сертифікат використовується за призначенням, відповідно до положень цієї Політики сертифіката.

### 9.6.4. Зобов'язання та гарантії суб'єктів, які довіряють КНЕДП – АЦСК МВС

Суб'єкт, який довіряє КНЕДП – АЦСК МВС, повинен перевірити чинність кваліфікованого сертифіката, сформованого КНЕДП – АЦСК МВС за допомогою програмного забезпечення для перевірки та підтвердження КЕП, перед використанням кваліфікованого сертифіката.

### 9.6.5. Зобов'язання та гарантії інших учасників

ЦЗО перш ніж прийняти рішення про внесення КНЕДП – АЦСК МВС до Довірчого списку та надання йому кваліфікованого статусу пересвідчився щодо наявності в КНЕДП – АЦСК МВС:

- документа, що підтверджує відповідність системи захисту інформації КНЕДП – АЦСК

МВС вимогам положень статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах»;

- документів, які підтверджують право власності та право користування КНЕДП – АЦСК МВС нежилими приміщеннями, які використовуються для розміщення всіх складових програмно-технічного комплексу, що забезпечують надання КЕД послуг;

- належного персоналу КНЕДП – АЦСК МВС;

- документів, які підтверджують освітньо-кваліфікаційний рівень та трирічний стаж роботи за фахом персоналу КНЕДП – АЦСК МВС;

- документів, які підтверджують право власності або право користування засобами КЕП, які використовуються КНЕДП – АЦСК МВС для надання КЕД послуг;

- документів, що підтверджують внесення коштів на поточний рахунок КНЕДП – АЦСК МВС із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) для забезпечення відшкодування збитків, які можуть бути заподіяні користувачам унаслідок неналежного виконання КНЕДП – АЦСК МВС своїх обов'язків;

- Регламента, цієї Політики сертифіката, Положень сертифікаційних практик;

- відомостей про ВПР КНЕДП та їхніх працівників, обов'язки яких будуть безпосередньо пов'язані з наданням КЕД довірчих послуг.

### 9.7. Відмова від гарантій

Не застосовується.

### 9.8. Обмеження відповідальності

У разі якщо КНЕДП – АЦСК МВС належним чином заздалегідь повідомить користувачів про обмеження щодо використання КЕД послуг, які він надає, за умови що такі обмеження є зрозумілими для користувачів, він не несе відповідальності за шкоду, завдану внаслідок використання КЕД послуг з порушенням зазначених обмежень.

### 9.9. Відшкодування збитків

Відшкодування збитків, які можуть бути завдані користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання КНЕДП – АЦСК МВС своїх зобов’язань здійснюється відповідно до вимог чинного законодавства України.

### 9.10. Термін дії та припинення дії

Ця Політика сертифіката застосовується з моменту її публікації та діє до закінчення строку дії останнього сертифіката, виданого відповідно до цієї Політики сертифіката або до моменту припинення діяльності КНЕДП – АЦСК МВС.

### 9.11. Індивідуальні повідомлення та комунікації з учасниками інфраструктури відкритих ключів

КНЕДП – АЦСК МВС здійснює комунікацію з учасниками інфраструктури відкритих ключів шляхом:

- розміщення повідомлень та оголошень на веб-сайті КНЕДП – АЦСК МВС;
- інформування ЦЗО, КО та органу з питань захисту персональних даних шляхом надсилання повідомлень в паперовій та електронній формах;

- консультування засобами поштового та телефонного зв’язку.

### 9.12. Зміни

Внесення змін до цієї Політики сертифіката здійснюється КНЕДП – АЦСК МВС у разі:

- змін вимог, процесів та процедур описаних в цій Політиці сертифіката;

- змін в законодавстві;

- змін у вимогах до КНЕДП щодо надання послуг.

Нові версії цієї Політики сертифіката після внесення змін до неї, публікуються на веб-сайті КНЕДП – АЦСК МВС.

Будь-які зміни, не зазначені в історії цієї Політики сертифіката, є граматичними і орфографічними змінами, які не впливають на суть та не стосуються процесів та процедур описаних в цій Політиці сертифіката.

### 9.13. Положення щодо вирішення спорів

У випадку виникнення спорів або розбіжностей, КНЕДП – АЦСК МВС вирішує їх шляхом переговорів та консультацій з учасниками інфраструктури відкритих ключів.

У разі недосягнення учасниками інфраструктури відкритих ключів згоди, спори (розбіжності) вирішуються у судовому порядку відповідно до чинного законодавства України.

### 9.14. Застосовне право

На відносини, що регулюються цією Політикою сертифіката, поширюється чинне законодавство України.

### 9.15. Дотримання чинного законодавства

Під час надання електронних довірчих послуг КНЕДП – АЦСК МВС повинен дотримуватися законодавства у сфері електронної ідентифікації, електронних довірчих послуг, захисту персональних даних та інформаційної безпеки:

– Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (із змінами (далі - Закон);

– Закону України «Про електронні документи та електронний документообіг» (із змінами);

– Закону України «Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань» (із змінами);

– Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»;

– постанови Кабінету Міністрів України від 28.06.2024 2024 № 764 «Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг»;

– постанови Кабінету Міністрів України від 01.08.2023 № 798 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності»;

– постанови Кабінету Міністрів України від 30.11.2016 № 869 «Про затвердження Порядку внесення засобів кваліфікованого електронного підпису до безконтактного електронного носія, що міститься в паспорті громадянина України, та надання кваліфікованих

електронних довірчих послуг з використанням паспорта громадянина України з імплантованим безконтактним електронним носієм» (зі змінами);

– постанови Кабінету Міністрів України від 23 липня 2024 р. № 842 «Про затвердження переліку документів та електронних даних, отриманих у зв'язку з наданням електронних довірчих послуг, що підлягають постійному зберіганню, та Порядку передачі обслуговування користувачів електронних довірчих послуг, з якими кваліфікований надавач електронних довірчих послуг, що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, уклав договори про надання кваліфікованих електронних довірчих послуг, до іншого кваліфікованого надавача електронних довірчих послуг»;

– постанови Кабінету Міністрів України від 10.12.2024 №1408 «Деякі питання зберігання документованої інформації та її передавання до центрального засвідчувального органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг»;

– наказу Міністерства внутрішніх справ України від 27.03.2018 № 238 «Про затвердження Порядку взаємодії акредитованого центру сертифікації ключів Міністерства внутрішніх справ України та Державної міграційної служби України під час надання послуг електронного цифрового підпису з використанням паспорта громадянина України з імплантованим безконтактним електронним носієм» (із змінами);

– наказу Міністерства цифрової трансформації України від 05.12.2022 року № 130 «Про затвердження Вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування», зареєстрованого в Міністерстві юстиції України 20 січня 2023 року за № 129/39185;

– інших нормативно-правових актів у сфері надання електронних довірчих послуг.