Додаток 2

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

ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

кваліфікованого надавача електронних довірчих послуг – акредитованого центру
сертифікації ключів міністерства внутрішніх справ України
щодо кваліфікованих сертифікатів електронного підпису та печатки

ЗМІСТ

1. ВСТУП

1.1. Огляд

Ці Положення сертифікаційних практик визначають перелік практичних дій та процедур щодо кваліфікованих сертифікатів електронного підпису та печатки (далі – кваліфіковані сертифікати) користувачів кваліфікованих електронних довірчих послуг (далі – КЕД послуги), зокрема, підписувачів та створювачів електронних печаток (далі – користувачі), які застосовуються кваліфікованим надавачем електронних довірчих послуг – акредитованим центром сертифікації ключів Міністерства внутрішніх справ України (далі – КНЕДП – АЦСК МВС) для реалізації Політики сертифіката кваліфікованого надавача електронних довірчих послуг МВС (додаток 1 до цього Регламенту) (далі – Політика сертифіката).

Дотримання практичних дій та процедур, визначених у цих Положеннях сертифікаційних практик, є обов'язковим для керівника КНЕДП – АЦСК МВС та працівників КНЕДП – АЦСК МВС, посадові обов'язки яких безпосередньо пов'язані з реєстрацією користувачів, формуванням та обслуговуванню їхніх кваліфікованих сертифікатів (далі - працівники), а також фізичних та юридичних осіб, які на підставі наказів МВС або договорів укладених з МВС безпосередньо чи опосередковано пов'язані з реєстрацією користувачів, формуванням та/або обслуговуванням їхніх кваліфікованих сертифікатів, зокрема, відокремлених пунктів реєстрації КНЕДП – АЦСК МВС (далі – ВПР КНЕДП – АЦСК МВС).

Визнання користувачами вимог, визначених у цих Положеннях сертифікаційних практик, є обов'язковою умовою та підставою для укладення з ними договору про надання КЕД послуг.

Перелік усіх правил, що застосовуються КНЕДП – АЦСК МВС у процесі реєстрації користувачів, формування та обслуговування кваліфікованих сертифікатів КНЕДП – АЦСК МВС та користувачів, зокрема управління їх статусом (блокування, поновлення та скасування) визначається Політикою сертифіката.

Ці Положення сертифікаційних практик відповідають вимогам, визначеним у:

- ДСТУ ETSI EN 319 411-1 (ETSI EN 319 411-1 V1.3.1, IDT) “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 V2.4.1, IDT) “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).

1.2. Назва документа та його ідентифікація

Відповідно до положення пункту 5.3 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

Повна назва документа: Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг – акредитованого центру сертифікації ключів Міністерства внутрішніх справ України щодо кваліфікованих сертифікатів електронного підпису та печатки.

Скорочена назва: Положення сертифікаційних практик.

Версія: 1.0.

OID: 1.2.804.2.1.1.1.2.2.

Ідентифікатор: NCP+ (пункт 5.3 (b) ETSI EN 319 411-1): Normalized Certificate Policy requiring a secure cryptographic device itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus(2).

1.3. Учасники інфраструктури відкритих ключів

Учасники інфраструктури відкритих ключів зазначені в пункту 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, що надає КЕД послуги з дотриманням вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги», зокрема, здійснює реєстрацію користувачів, формування та обслуговування їхніх кваліфікованих сертифікатів, у тому числі, управління їхнім статусом (блокування, поновлення та скасування), управління парою ключів від імені підписувача чи створювача електронної печатки.

КНЕДП – АЦСК МВС здійснює реєстрацію користувачів самостійно та/або через ВПР КНЕДП – АЦСК МВС, а також уповноваженими працівниками ДМС на здійснення представництва КНЕДП – АЦСК МВС під час надання КЕД послуг з використанням паспорта громадянина України з імплантованим безконтактним електронним носієм (далі – уповноважені працівники ДМС).

Пункт 1.3.1 Політики сертифіката містить додаткову інформацію.

1.3.2. Органи реєстрації

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 надання КЕД послуг.

Безпосередню реєстрацію користувача у ВПР КНЕДП – АЦСК МВС здійснює працівник ВПР КНЕДП – АЦСК МВС, на якого покладено відповідні обов'язки з реєстрації користувачів (далі - віддалений адміністратор реєстрації).

До працівників ВПР КНЕДП – АЦСК МВС, на яких покладено обов'язки з реєстрації користувачів, та уповноважені працівники ДМС застосовуються такі ж вимоги, як і до адміністраторів реєстрації, що визначені у пункті 5.3.2. Політики сертифіката.

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, а саме:

1) підписувачі:
- фізичні особи - резиденти;
- фізичні особи - нерезиденти;
- самозайняті особи (нотаріуси, адвокати, арбітражні керуючі, приватні виконавці, тощо);
- посадові особи (наймані працівники, підрядники тощо) юридичної особи, представництва юридичної особи - нерезидента, посадові особи юридичної особи - нерезидента, фізичної особи - підприємця, самозайнятої особи;

2) створювачі електронних печаток:
- юридичні особи - резиденти;
- представництва юридичних осіб - нерезидентів;
- фізичні особи - підприємці.

Політика сертифіката містить додаткову інформацію.

1.3.4. Суб'єкти, які довіряють

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 електронного підпису чи печатки.

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.

Політика сертифіката містить додаткову інформацію.

1.4. Використання сертифіката

Використання сертифікатів відповідає положенням пункту 5.5 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

1.4.1. Дозволене використання сертифіката

Кваліфіковані сертифікати, сформовані КНЕДП – АЦСК МВС, дозволено використовувати для:

- автентифікації;
- створення, перевірки та підтвердження кваліфікованого електронного підпису;
- створення, перевірки та підтвердження кваліфікованої електронної печатки;
- узгодження ключів шифрування.

Усі кваліфіковані сертифікати, сформовані КНЕДП – АЦСК МВС, у розширенні « qualified certificate statement» містять значення:

1.2.804.2.1.1.1.2.2 - для особистих ключів, що зберігаються в засобі КЕП.

КНЕДП – АЦСК МВС для визначення сфери використання кваліфікованого сертифіката користувача, під час його формування встановлює розширення сертифіката "Призначення відкритого ключа" ("keyUsage"), зазначені у Таблиці 1.

Таблиця 1. Розширення сертифіката, що вносяться до кваліфікованого сертифіката для визначення його сфери використання

Сфера використання кваліфікованого сертифіката	**Розширення сертифіката "Призначення відкритого ключа" ("keyUsage")**
Автентифікація	digitalSignature + nonRepudiation або keyAgreement

Створення, перевірка та підтвердження кваліфікованого електронного підпису	digitalSignature + nonRepudiation
Створення, перевірка та підтвердження кваліфікованої електронної печатки	digitalSignature + nonRepudiation
Узгодження ключів шифрування	keyAgreement

КНЕДП – АЦСК МВС формує кваліфіковані сертифікати з розширеннями сертифіката “digitalSignature + nonRepudiation” або “keyAgreement” за умов, що такі відкриті ключі належать до різних ключових пар.

КНЕДП – АЦСК МВС для визначення сфери використання кваліфікованого сертифіката користувача як кваліфікованого сертифіката електронної печатки під час його формування встановлює додаткове розширення “Уточнене призначення відкритого ключа” (“extendedKeyUsage”) із об’єктним ідентифікатором (OID): 1.2.804.2.1.1.1.3.9.

У випадках, коли вимогами до деяких інформаційно-комунікаційних систем встановлено, що автентифікація в них може здійснюватися лише з використанням кваліфікованого сертифіката, особистий ключ якого було згенеровано із застосування засобу КЕП (id-etsi-qcs 4), КНЕДП – АЦСК МВС під час формування відповідного кваліфікованого сертифіката встановлює додаткове розширення “Уточнене призначення відкритого ключа” (“extendedKeyUsage”) та умовне позначення типу такого носія у додаткових даних користувача для ідентифікації типу такого засобу КЕП. Таке розширення застосовується лише в кваліфікованих сертифікатах, особисті ключі яких згенеровані відповідно до ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”, затвердженого наказом Державного комітету з питань технічного регулювання та споживчої політики від 28 грудня 2002 р. № 31.

1.4.1.1. Види сертифікатів

Відповідно до цих Положень сертифікаційних практик КНЕДП – АЦСК МВС формує кваліфіковані сертифікати таких типів:

- 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 КЕП з фізичною особою, юридичною особою або фізичною особою - підприємцем та забезпечує направлене шифрування під час обміну інформацією.

1.4.1.2. Строк дії сертифікатів

Кваліфіковані сертифікати користувачів формуються КНЕДП – АЦСК МВС зі строком дії, що не перевищує 2 роки.

1.4.2. Заборонене використання сертифіката

Не допускається використання кваліфікованого сертифіката, сформованого КНЕДП – АЦСК МВС, у сферах, які не відповідають зазначеному у кваліфікованому сертифікаті призначенню відкритого ключа (“keyUsage”).

1.5. Управління Положеннями сертифікаційних практик

1.5.1. Відповідальність за Положення сертифікаційних практик

Ці Положення сертифікаційних практик підтримуються Міністерством внутрішніх справ України. Міністерство внутрішніх справ України є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України. Головний офіс КНЕДП – АЦСК МВС представлений Департаментом інформатизації, що забезпечує надання КНЕДП – АЦСК МВС кваліфікованих електронних довірчих послуг, організацію використання кваліфікованих електронних довірчих послуг у МВС. Структурний підрозділ Департаменту інформатизації здійснює організацію надання кваліфікованих електронних довірчих послуг відокремленими пунктами реєстрації КНЕДП – АЦСК МВС та забезпечує виконання вимог законодавства до КНЕДП.

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

Реквізити Міністерства внутрішніх справ України:

- Код згідно з Єдиним державним реєстром підприємств та організацій України (ЄДРПОУ): 00032684.

- Адреса: вул. Богомольця Академіка, 10, м. Київ, 00024, Україна.

- Контактний телефон: +38 (044) 256-03-33.

Реквізити КНЕДП – АЦСК МВС :

- Адреса веб-сайту: https://ca.mvs.gov.ua/.

- Контактний телефон: +38 (044) 254-77-55.

- Адреса електронної пошти: ca@mvs.gov.ua.

Ці Положення сертифікаційних практик структуровані відповідно до RFC 3647 «Інфраструктура відкритих ключів Інтернету X.509 Політика сертифікації та структура практики сертифікації», ДСТУ ETSI EN 319 401:2022 (ETSI EN 319 401 V2.3.1 (2021-05), IDT) «Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг», ДСТУ ETSI EN 319 411-1:2022 (ETSI EN 319 411-1 V1.3.1 (2021-05), IDT «Електронні підписи та інфраструктури (ESI) і містить всю необхідну інформацію

Ці Положення сертифікаційних практик та зміни до них підписуються керівником КНЕДП – АЦСК МВС, який відповідає за дотримання, визначених у них практичних дій та процедур, та затверджуються Міністром внутрішніх справ України.

Ці Положення сертифікаційних практик та зміни до них погоджуються Міністерством цифрової трансформації України, яке направляє їхні копії до Адміністрації Державної служби спеціального зв’язку та захисту інформації України.

1.5.2. Внесення змін до Положення сертифікаційних практик

Відповідно до пункту 9.12 Положення сертифікаційних практик.

Зміни до Положення сертифікаційних практик вносяться у порядку, передбаченому законодавством для внесення змін до Регламенту.

1.6. Визначення термінів та перелік скорочень

1.6.1. Визначення термінів

У цих Положеннях сертифікаційних практик 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», постановах Кабінету Міністрів України від 28.06.2024 р. № 764 «Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг» (зі змінами), інших нормативно-правових актах у сферах електронних довірчих послуг, криптографічного та технічного захисту інформації, електронних комунікацій.

1.6.2. Перелік скорочень

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
засіб КЕП	засіб кваліфікованого електронного підпису чи печатки
ІКС	Інформаційно-комунікаційна система
КЗІ	Криптографічний захист інформації
КНЕДП	Кваліфікований надавач електронних довірчих послуг
КО	Контролюючий орган (Адміністрація державної служби спеціального зв'язку та захисту інформації України)
ООВ	Орган з оцінки відповідності
ПТК	Програмно-технічний комплекс
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

Згідно з положеннями пункту 6.1 ETSI EN 319 411-1 та пункту 6.1 ETSI EN 319 411-2.

2.1. Репозиторій / веб-сайт

КНЕДП – АЦСК МВС через веб-сайт (https://ca.mvs.gov.ua/) забезпечує вільний доступ до:

- загальних відомості про КНЕДП – АЦСК МВС (у тому числі про його ВПР та виїзних адміністраторів реєстрації);
- даних про внесення відомостей про КНЕДП – АЦСК МВС до Довірчого списку;
- текстів Регламенту, Політики сертифіката та Положень сертифікаційних практик (крім розділів, що не входить до обсягу положень, визначених КНЕДП – АЦСК МВС для ознайомлення користувачами);
- переліку КЕД послуг, які надає КНЕДП – АЦСК МВС ;
- текст договору про надання КЕД послуг;
- кваліфікованих сертифікатів ЦЗО;
- кваліфікованих сертифікатів КНЕДП – АЦСК МВС, серверів КНЕДП – АЦСК МВС (OCSP, TSP, CMP);
- загальних положень та умов надання КЕД послуг користувачам КНЕДП – АЦСК МВС ;
- кваліфікованих сертифікатів Користувачів, які надали згоду на їх публікацію, та підписувачів – володільців паспорта громадянина України з імплантованим БЕН;
- даних про засоби КЕП (QSCD), що використовуються під час надання КЕД послуг КНЕДП – АЦСК МВС ;
- реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;
- відомостей про обмеження під час використання кваліфікованих сертифікатів Користувачами;
- даних про порядок перевірки чинності кваліфікованого сертифіката, у тому числі умови перевірки статусу кваліфікованого сертифіката;
- переліку нормативно-правових актів у сфері надання КЕД послуг;
- даних про засоби КЕП, що використовуються під час надання КЕД послуг;
- форми заяв, які подаються до КНЕДП – АЦСК МВС для отримання КЕД послуг, приклади їх заповнення та рекомендації щодо порядку подання таких заяв та отримання КЕД послуг.

Ці Положення сертифікаційних практик доступні цілодобово на офіційному веб-сайті КНЕДП – АЦСК МВС (https://ca.mvs.gov.ua/).

КНЕДП – АЦСК МВС забезпечує регулярне оновлення інформації та публікацію кваліфікованих сертифікатів, Регламенту роботи кваліфікованого надавача електронних довірчих послуг - акредитованого центру сертифікації ключів Міністерства внутрішніх справ України (далі – Регламент), Політики сертифіката, Положень сертифікаційних практик, списків відкликаних сертифікатів, договорів, актів законодавства та інших нормативних документів на офіційному веб-сайті КНЕДП – АЦСК МВС.

2.2. Публікація інформації

2.2.1. Публікація сертифікатів користувачів

ПТК КНЕДП – АЦСК МВС забезпечує публікацію кваліфікованих сертифікатів користувачів, згода на публікацію яких надана такими користувачами, та списків відкликаних сертифікатів (CRL) на веб-сайті КНЕДП – АЦСК МВС.

Кваліфіковані сертифікати користувачів, які надали згоду на їх публікацію, публікуються одразу після формування таких кваліфікованих сертифікатів.

Публікація кваліфікованих сертифікатів, сформованих користувачу, на ім'я якого оформлено паспорт громадянина України з імплантованим БЕН, на який згенеровано перші пари ключів, здійснюється автоматично на офіційному веб-сайті КНЕДП – АЦСК МВС.

2.2.2. Публікація сертифікатів КНЕДП – АЦСК МВС

КНЕДП – АЦСК МВС забезпечує вільний доступ до інформації про кваліфіковані сертифікати КНЕДП – АЦСК МВС через власний веб-сайт (https://ca.mvs.gov.ua/).

Кваліфіковані сертифікати КНЕДП – АЦСК МВС та серверів КНЕДП – АЦСК МВС публікуються одразу після їх формування або отримання від ЦЗО.

Відомості про кваліфіковані сертифікати КНЕДП – АЦСК МВС, сформовані з використанням самопідписаного сертифіката електронної печатки ЦЗО, статус та обмеження у використанні таких сертифікатів, а також CRL містяться в реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів, що ведеться ЦЗО (https://czo.gov.ua/).

2.2.3. Доступ до сертифікатів користувачів

КНЕДП – АЦСК МВС забезпечує цілодобовий доступ користувачів до їхніх власних кваліфікованих сертифікатів. Доступ інших осіб до кваліфікованих сертифікатів користувачів надається за умови надання такими користувачами згоди на публікацію їх кваліфікованих сертифікатів та закінчення строку, на який було введено воєнний стан в Україні.

2.2.4. Строк закінчення дії сертифіката

Строк дії кваліфікованих сертифікатів користувачів становить не більше двох років.

Дата та час початку та закінчення строку дії кваліфікованого сертифіката користувачів зазначається у кваліфікованому сертифікаті.

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

2.3. Час та періодичність публікації

КНЕДП – АЦСК МВС формує списки відкликаних сертифікатів 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 кваліфікований електронний підпис чи печатка КНЕДП – АЦСК МВС.

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

Час зміни статусу кваліфікованих сертифікатів синхронізований із Всесвітнім координованим часом (UTC) з точністю до однієї секунди. Посилання на списки відкликаних сертифікатів вносяться до кваліфікованих сертифікатів Користувачів.

КНЕДП – АЦСК МВС формує списки відкликаних сертифікатів у вигляді повного та часткового списків.

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

2.4. Контроль доступу до репозиторію/веб-сайту

Кваліфіковані сертифікати КНЕДП – АЦСК МВС та користувачів, списки відкликаних сертифікатів, Регламент, відповідні Положення сертифікаційних практик та Політики сертифіката доступні у репозиторії/веб-сайті цілодобово. Доступ лише для читання необмежений. Зміни у репозиторії/веб-сайті здійснюються виключно КНЕДП – АЦСК МВС.

Користувач може знайти інформацію про свій кваліфікований сертифікат шляхом здійснення його пошуку на веб-сайті КНЕДП – АЦСК МВС, заповнивши у відповідних вкладках дані РНОКПП (у разі відсутності серія (за наявності) та номер паспорта) або УНЗР.

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, які формує КНЕДП – АЦСК МВС обов'язково повинні містити відомості, визначені частиною другою статті 23 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», а саме:

1) позначку (у формі, придатній для автоматизованої обробки) про те, що сертифікат виданий як кваліфікований сертифікат;
2) позначку, що сертифікат виданий в Україні;
3) ідентифікаційні дані, які однозначно визначають КНЕДП – АЦСК МВС, у тому числі обов’язково найменування та код згідно з ЄДРПОУ;
4) ідентифікаційні дані, які однозначно визначають користувача, у тому числі обов’язково:

- прізвище, власне ім’я, по батькові (за наявності) підписувача та УНЗР або РНОКПП, або серію (за наявності) та номер паспорта громадянина України (для фізичних осіб, які мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта), або номер паспортного документа іноземця чи особи без громадянства;
- найменування або прізвище, власне ім’я, по батькові (за наявності) створювача електронної печатки та код згідно з ЄДРПОУ (код/номер з торговельного, банківського чи судового реєстру, що ведеться країною резидентства іноземної юридичної особи, код/номер з реєстраційного посвідчення місцевого органу влади іноземної держави про реєстрацію юридичної особи), крім 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, або УНЗР, або РНОКПП, або серію (за наявності) та номер паспорта громадянина України (для фізичних осіб, які мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта);

5) значення відкритого ключа, який відповідає особистому ключу;
6) відомості про початок та закінчення строку дії кваліфікованого сертифіката;
7) серійний номер кваліфікованого сертифіката, унікальний для КНЕДП – АЦСК МВС;

8) кваліфікований електронний підпис або кваліфіковану електронну печатку, створені КНЕДП – АЦСК МВС;

9) відомості про місце надання послуги перевірки статусу відповідного кваліфікованого сертифіката;

10) зазначення про те, що особистий ключ, пов’язаний з відкритим ключем, зберігається в засобі КЕП, - у формі, придатній для автоматизованої обробки.

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 Політики сертифіката. Позначення, що використовуються в кваліфікованих сертифікатах користувачів, наведені в Таблиці 2.

Таблиця 2. Позначення, що використовуються в кваліфікованих сертифікатах користувачів

Найменування	Значення
Country (C)	Назва країни 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
Organization (O)	Найменування юридичної особи для кваліфікованих сертифікатів електронних печаток юридичної особи або кваліфікованих сертифікатів представника юридичної особи. Для кваліфікованих сертифікатів фізичних осіб, які не належать до юридичної особи, це поле недоступне
Organizational Unit (OU)	Назва підрозділу або відділу в організації. Для кваліфікованих сертифікатів фізичних осіб, які не належать до юридичної особи, це поле недоступне
State or Province (ST)	Назва області місцезнаходження або місця реєстрації користувача
Title (T)	Посада (для кваліфікованих сертифікатів представників юридичної особи за необхідності)
Locality (L)	Назва населеного пункту місцезнаходження або місця реєстрації користувача

Common Name (CN)	Повне ім’я (найменування) користувача, якому належить кваліфікований сертифікат
Surname (SN)	Прізвище користувача, якому належить кваліфікований сертифікат
GivenName (G)	Власне ім’я, по батькові (за наявності) користувача, якому належить кваліфікований сертифікат
Serial=TINUA	РНОКПП користувача, якому належить кваліфікований сертифікат або серія (за наявності) та номер паспорта
OI =NTRUA	Код ЄДРПОУ юридичної особи для кваліфікованого сертифіката юридичної особи або кваліфікованого сертифіката представника юридичної особи
E-Mail Address (E)	Електронна пошта користувача, якому належить кваліфікований сертифікат

3.1.1. Типи позначень сертифіката

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 Політики сертифіката.

3.1.2. Позначення (реквізити та атрибути) сертифікатів

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

3.1.3. Анонімність або використання псевдонімів

Не застосовується.

3.1.4. Правила інтерпретації різних форм позначень сертифіката

Міжнародні літери повинні кодуватися згідно з UTF-8.

3.1.5. Унікальність позначень сертифіката

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 особи

Для отримання КЕД послуг особа, яка звернулася до КНЕДП – АЦСК МВС, повинна бути встановлена (ідентифікована, автентифікована) відповідно до вимог законодавства у сферах надання КЕД послуг та електронної ідентифікації і Регламенту.

Ідентифікація, автентифікація користувачів (у тому числі уповноважених посадових осіб, відповідальних за застосування електронної печатки) здійснюється КНЕДП – АЦСК МВС у випадках:

- звернення до КНЕДП – АЦСК МВС із заявою про реєстрацію;
- звернення до КНЕДП – АЦСК МВС із заявою на зміну статусу сертифіката (скасування, блокування, поновлення сертифіката), повторне формування сертифіката.

Підстави відмови у наданні КЕД послуг:

- відсутність повного пакету документів, або інших відомостей, у тому числі в електронній формі, необхідних для ідентифікації чи автентифікації користувачів;
- подання документів, що мають підчистки, дописи, закреслені слова, інші виправлення, написи олівцем або мають пошкодження, внаслідок чого їх текст неможливо прочитати;
- у заяві відсутня інформація, необхідна для формування або зміни статусу кваліфікованого сертифіката;
- форма заяви не відповідає встановленому зразку;
- заява оформлена неналежним чином;
- строк подання заяви та пакету документів перевищив п’ять робочих днів з дня їх підписання та/або завірення;
- подання неналежно засвідчених копій документів;
- встановлення невідповідності даних, що визначені наданими документами, або іншими відомостями, у тому числі в електронній формі, фактичним даним;
- відсутність у користувача засобу КЕП або виявлення при формуванні кваліфікованого сертифіката відсутності відмітки про те, що ключову пару згенеровано в засобі КЕП;
- неунікальність наданого відкритого ключа користувача в реєстрі чинних, блокованих та скасованих сертифікатів.

Користувач повинен надати номер телефону та/або адресу електронної пошти для отримання можливості КНЕДП – АЦСК МВС зв’язатися з ними у випадку необхідності.

За наявності технічної можливості, додаткова ідентифікація користувачів може здійснюватися з використанням даних, одержаних з інформаційних систем органів державної влади (реєстрів, баз даних тощо) в електронному вигляді.

Копії паперових документів, що подаються КНЕДП – АЦСК МВС для отримання КЕД послуг, засвідчуються відповідно до законодавства.

Перелік документів та рекомендації щодо їх оформлення публікуються на офіційному веб-сайті КНЕДП – АЦСК МВС.

З метою укладання договорів про надання КЕД послуг КНЕДП – АЦСК МВС може отримувати від користувачів документи та інформацію, передбачені законодавством.

Перед отриманням КЕД послуг користувачу необхідно ознайомитися з Регламентом та Договором про надання кваліфікованих електронних довірчих послуг, розміщених на офіційному веб-сайті КНЕДП – АЦСК МВС.

У випадку негативної ідентифікації чи автентифікації або відмови в розгляді заяв про реєстрацію чи зміну статусу сертифіката з причин, що наведено вище, всі документи, що були надані на розгляд, повертаються заявнику.

3.2.1. Механізм підтвердження володіння особистим ключем

Пункт 3.2.1. Політики сертифіката містить інформацію щодо механізмів підтвердження володіння користувачем особистим ключем.

3.2.2. Ідентифікація та автентифікація юридичної особи

Для ідентифікації юридичної особи, уповноважений працівник якої звернувся до КНЕДП – АЦСК МВС для отримання КЕД послуг, КНЕДП – АЦСК МВС вимагає разом із заявою надати, а юридична особа надає ідентифікаційні дані, що вносяться до кваліфікованого сертифіката.

Перелік ідентифікаційних даних юридичної особи, що вносяться до кваліфікованого сертифіката, та механізми їх підтвердження визначається у Таблиці 3.

Таблиця 3. Ідентифікаційні дані та механізми їх підтвердження під час встановлення юридичних осіб, уповноважені працівники яких звернулися за отриманням КЕД послуги

Ідентифікаційні дані	**Обов'язковість надання ідентифікаційних даних**	**Механізми підтвердження ідентифікаційних даних**
Повне та скорочене (за наявності) найменування юридичної особи	Обов'язково	Документальне (отримання витягу з ЄДР у паперовому вигляді) або технічне (отримання інформації в електронній формі з ЄДР)
Код згідно з ЄДРПОУ	Обов'язково	Документальне (отримання витягу з ЄДР у паперовому вигляді) або технічне (отримання інформації в електронній формі з ЄДР)
Місцезнаходження	За необхідності	Документальне (отримання витягу з ЄДР у паперовому вигляді) або технічне (отримання інформації в електронній формі з ЄДР)

3.2.3. Ідентифікація та автентифікація фізичних осіб

3.2.3.1. Ідентифікація фізичних осіб

Для ідентифікації користувача (фізичної особи, фізичної особи – представника юридичної особи), яка звернулася до КНЕДП – АЦСК МВС для отримання КЕД послуг, КНЕДП – АЦСК МВС вимагає разом із заявою надати, а користувач надає ідентифікаційні дані, що вносяться до кваліфікованого сертифіката. Перелік ідентифікаційних даних, що вносяться до кваліфікованого сертифіката, та механізми їх підтвердження визначається у Таблиці 4.

Таблиця 4. Ідентифікаційні дані та механізми їх підтвердження під час встановлення фізичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката

Ідентифікаційні дані	Обов'язковість надання ідентифікаційних даних	Механізми підтвердження ідентифікаційних даних
Прізвище, ім'я, по батькові (за наявності)	Обов'язково	Документальне або електронне (паспорт,

		посвідка на постійне (тимчасове) місце проживання)
РНОКПП	За наявності	Документальне або електронне (облікова картка платника податків, паспорт)
Серія (за наявності), номер паспорта	Обов'язково для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та офіційно повідомили про це відповідний податковий орган і мають відмітку або інформацію в паспорті громадянина України про право здійснювати будь-які платежі за серією та/або номером паспорта	Документальне або електронне (паспорт)
УНЗР	На вимогу користувача про їх включення до кваліфікованого сертифіката	Документальне або електронне (паспорт)
Номер телефону	Обов'язково	
Адреса електронної пошти	На вимогу користувача про її включення до кваліфікованого сертифіката	
Підрозділ	На вимогу користувача про їх включення до кваліфікованого сертифіката	Документальне (документ, що засвідчує право на здійснення діяльності у визначеній сфері: посвідчення, сертифікат, наказ про призначення, свідоцтво тощо)
Повноваження або займана посада	На вимогу користувача про їх включення до кваліфікованого сертифіката.	Документальне (документ, що засвідчує право на здійснення діяльності у визначеній сфері: посвідчення, сертифікат, наказ про призначення, свідоцтво тощо)
Назва та номер документа, що підтверджує право самозайнятої особи на	На вимогу користувача про їх включення до кваліфікованого сертифіката	Документальне (документ, що засвідчує право на здійснення діяльності у

здійснення діяльності у певній сфері		визначеній сфері: посвідчення, сертифікат, наказ про призначення, свідоцтво тощо)
Назва держави, населеного пункту, адреса, інформація про які міститься у відомостях про місце проживання (перебування) фізичної особи	На вимогу користувача про їх включення до кваліфікованого сертифіката	Документальне або електронне (паспорт, посвідка на постійне (тимчасове) місце проживання, Витяг з реєстру територіальної громади)

Ідентифікація фізичних осіб - нерезидентів, які особисто звертаються до КНЕДП – АЦСК МВС для отримання КЕД послуг, здійснюється за документами, що підтверджують ідентифікаційні дані фізичних осіб - нерезидентів. Якщо текст у документах викладений іноземною мовою, разом з копіями таких документів надається переклад українською мовою, засвідчений нотаріально.

Приймання заяв про реєстрацію в КНЕДП – АЦСК МВС як підписувачів, ідентифікація підписувачів при наданні КЕД послуг особі, на ім’я якої оформлено паспорт громадянина України з імплантованим БЕН, при генерації на БЕН першої пари ключів проводиться працівниками суб'єктів, уповноважених на видачу паспорта громадянина України з імплантованим БЕН (зокрема територіальних органів та територіальних підрозділів ДМС), які здійснюють представництво КНЕДП – АЦСК МВС відповідно до законодавства України.

Форми документів, на підставі яких надаються КЕД послуги, та рекомендації щодо їх оформлення публікуються на веб-сайті КНЕДП – АЦСК МВС.

Для укладання договорів про надання КЕД послуг КНЕДП – АЦСК МВС може отримувати від користувачів інші документи, передбачені законодавством. Заяви та копії документів, що використовувались під час ідентифікації користувача, засвідчуються за правилами, наведеними у Таблиці 5.

Таблиця 5. Правила засвідчення документів, що використовувались під час ідентифікації користувача.

Форма документа	**Засвідчення з боку користувача**		**Засвідчення з боку КНЕДП – АЦСК МВС (адміністратор реєстрації)**	
	Тип підпису	**Черга засвідчення**	**Тип підпису**	**Черга засвідчення**
Паперова	Власноручний підпис підписувача та/або уповноваженого представника юридичної особи/ створювача	Перша	Власноручний підпис та штамп адміністратора реєстрації на заяві.	Друга

	електронної печатки			
Електронна	Кваліфікований електронний підпис та/або кваліфікована електронна печатка	Перша	Кваліфікований електронний підпис адміністратора реєстрації реєстрації на електронному документі.	Друга

Перевірка відомостей (даних) про особу 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, здійснюється одним із таких способів:

- без залучення додаткових пристроїв шляхом візуального зіставлення однакової інформації (значення "УНЗР", серія (за наявності), номер паспорта, строк дії), яка надрукована в зоні візуальної перевірки та машинозчитувальній зоні;

- засобами Єдиного державного веб порталу електронних послуг (Портал Дія) шляхом передачі за бажанням особи електронної копії е-паспорта або е-паспорта для виїзду за кордон до ІКС КНЕДП – АЦСК МВС.

Під час ідентифікації користувача 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, здійснюється перевірка дійсності таких документів з використанням відомостей інформаційних ресурсів ЄІС МВС (відомостей, що містяться в ЄДДР, та відомостей щодо викрадених (втрачених) документів - за зверненнями громадян).

3.2.4. Неперевірена інформація про користувача

Ідентифікація особи здійснюється КНЕДП – АЦСК МВС, ВПР КНЕДП – АЦСК МВС шляхом перевірки та підтвердження належності фізичній чи юридичній особі, яка звернулася за отриманням послуги формування кваліфікованого сертифіката, ідентифікаційних даних особи, отриманих КНЕДП – АЦСК МВС, ВПР КНЕДП – АЦСК МВС).

3.2.5. Підтвердження повноважень

Під час ідентифікації уповноваженого представника юридичної особи або фізичної особи - підприємця КНЕДП – АЦСК МВС здійснює автентифікацію такого користувача відповідно до пункту 3.2.2 цих Положень сертифікаційних практик перевіряє обсяг 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. Якщо від імені юридичної особи діє колегіальний орган, до КНЕДП – АЦСК МВС подається документ, у якому визначено повноваження відповідного органу та розподіл обов'язків між його членами.

Ідентифікація (встановлення) юридичних осіб та фізичних осіб – представників юридичних осіб (керівників органів управління, посадових осіб, працівників, співробітників тощо), які особисто звертаються до КНЕДП – АЦСК МВС для отримання КЕД послуг, здійснюється за документами або іншими відомостями, у тому числі в електронній формі, що

підтверджують ідентифікаційні дані юридичних осіб та фізичних осіб – представників юридичних осіб.

Для встановлення належності фізичних осіб до юридичної особи та їх повноважень, у тому числі як відповідального працівника державної установи за організацію КЕД послуг у цій установі, використовуються:

- оригінали (для ознайомлення) та копії документів, що посвідчують особу та підтверджують її ідентифікаційні дані;
- копії документів, що посвідчують особу керівника юридичної особи та підтверджують її ідентифікаційні дані;
- копії документів, що підтверджують повноваження керівника юридичної особи;
- копії документів, що підтверджують повноваження (займану посаду) особи;
- оригінали (для ознайомлення) та копії документів, що посвідчують особу уповноваженого представника створювача електронної печатки та підтверджують його повноваження.

3.3. Ідентифікація та автентифікація за заявою для повторного формування кваліфікованих сертифікатів відкритого ключа

Під час повторного формування кваліфікованого сертифіката користувача КНЕДП – АЦСК МВС повинен перевірити актуальність інформації, що надавалася для попереднього формування кваліфікованого сертифіката.

У разі зміни відомостей, що містяться у кваліфікованому сертифікаті, користувач у триденний строк з дня настання таких змін повідомляє про це КНЕДП – АЦСК МВС та надає заяву та документи, що підтверджують відповідні зміни. На підставі наданих користувачем документів, що підтверджують зміни відомостей, що містяться у кваліфікованому сертифікаті, КНЕДП – АЦСК МВС здійснює повторне формування такого сертифіката та його публікацію у разі згоди користувача.

Автентифікація користувачів, які мають чинний кваліфікований сертифікат, сформований КНЕДП – АЦСК МВС, може здійснюватися у випадку подання в електронній формі заяв про формування, блокування та скасування кваліфікованих сертифікатів, у разі незмінності ідентифікаційних даних внесених до попереднього кваліфікованого сертифіката з моменту формування сертифіката до моменту створення кваліфікованого електронного підпису на заяві.

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

Повторне формування кваліфікованого сертифіката користувача не продовжує строку його дії.

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

Перелік та опис механізмів автентифікації користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката наводиться в Таблиці 6.

Таблиця 6. Перелік та опис механізмів автентифікації користувачів щодо

блокування, скасування або поновлення кваліфікованого сертифіката.

Тип операції (причина подання заяв)	**Форма подання заяв**	**Механізми підтвердження ідентифікаційних даних**
Блокування кваліфікованого сертифіката	Усна	За ключовою фразою голосової автентифікації, що зазначається у заяві для формування кваліфікованого сертифіката, та ідентифікаційними даними, вказаними в кваліфікованому сертифікаті
	Письмова паперова	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката
	Письмова електронна	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які мають чинний кваліфікований сертифікат, сформований КНЕДП – АЦСК МВС
Скасування кваліфікованого сертифіката	Письмова паперова	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката
	Письмова електронна	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які мають чинний кваліфікований сертифікат, сформований КНЕДП – АЦСК МВС
Поновлення кваліфікованого сертифіката	Письмова паперова	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які вперше звернулися за отриманням

		послуги формування кваліфікованого сертифіката

3.5. Автентифікація при втраті засобу автентифікації

КНЕДП – АЦСК МВС не використовує номер телефону та адресу електронної пошти користувача як засоби автентифікації користувача для подання заяв про блокування або скасування кваліфікованого сертифіката. Автентифікація користувача здійснюється за допомогою усного звернення до КНЕДП – АЦСК МВ, зокрема із зазначенням ідентифікаційних даних підписувача, ключової фрази голосової автентифікації.

4. ОПЕРАЦІЙНІ 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 на формування кваліфікованого сертифіката

До суб'єктів, уповноважених подавати заяву на формування кваліфікованого сертифіката, належать користувачі, що пройшли процедури ідентифікації та автентифікації.

Заяви на отримання КЕД послуг заповнюються українською мовою друкованими літерами та цифрами кульковою ручкою або в електронному вигляді з подальшим їх роздрукуванням та підписанням кульковою ручкою, проставленням печатки (за наявності).

Заяви не повинні містити дописи, виправлення, написи олівцем або мати пошкодження бланку, які унеможливлюють прочитання тексту. Використання факсимільного відтворення підписів при оформленні заяв не допускається.

Копії документів та витяги з них, що подаються на реєстрацію разом із заявою, крім нотаріально засвідчених, засвідчуються відповідно до чинного законодавства.

Заява та пакет документів подаються КНЕДП – АЦСК МВС не пізніше п'яти робочих днів з дня підписання заяви та завірення копій документів.

У разі позитивної ідентифікації оригінали документів, що були надані особою під час реєстрації для ознайомлення, повертаються їй.

У випадку позитивної ідентифікації адміністратор реєстрації (віддалений адміністратор реєстрації) КНЕДП – АЦСК МВС вносить ідентифікаційні дані Користувача до реєстру користувачів КНЕДП – АЦСК МВС (здійснює реєстрацію). У випадку проведення виїзної генерації ключів адміністратор реєстрації проводить ідентифікацію, автентифікацію Користувачів за їх місцем знаходження та у разі позитивного результату передає їх ідентифікаційні дані (у тому числі зображення оригіналів документів) та запити на сертифікацію в електронному вигляді з використанням засобів КЗІ (шифрування) віддаленому адміністратору реєстрації, який знаходиться в приміщенні ВПР КНЕДП – АЦСК МВС, для здійснення ним перевірки даних, реєстрації Користувача та передачі запитів на сертифікацію до КНЕДП – АЦСК МВС. Працівники КНЕДП – АЦСК МВС, які здійснили виїзну ідентифікацію, відповідають за передачу заяв про реєстрацію, про зміну статусу кваліфікованих сертифікатів, пакетів документів до них у паперовому та / або електронному вигляді, а також запитів на сертифікацію до КНЕДП – АЦСК МВС (із забезпеченням цілісності та відповідності даних документам, на підставі яких здійснено ідентифікацію).

Для підтвердження ідентифікаційних даних уповноваженого представника юридичної особи КНЕДП – АЦСК МВС використовує результати перевірки відомостей (даних) про особу, отримані 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.

У разі відсутності в іноземців та осіб без громадянства документів, що підтверджують ідентифікаційні дані, виданих відповідно до законодавства про ЄДДР та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи, їх ідентифікація здійснюється за легалізованим належним чином паспортним документом іноземця або документом, що посвідчує особу без громадянства.

Якщо від імені юридичної особи діє колегіальний орган, КНЕДП – АЦСК МВС, в якому визначено повноваження такого органу та розподіл обов'язків між його членами.

Ідентифікація особи здійснюється шляхом перевірки наданих нею ідентифікаційних даних, зокрема тих, що включаються до кваліфікованого сертифіката, та її повноважень, на підставі наданих документів або даних, одержаних 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 (паспортом громадянина іншої країни із нотаріально засвідченим перекладом на українську мову, посвідкою на тимчасове/постійне проживання, посвідченням біженця або паспортом громадянина України для виїзду за кордон тощо).

Під час ідентифікації особи КНЕДП – АЦСК МВС використовуються наявні сервіси перевірки чинності документів та ідентифікаційної інформації про особу, зокрема сервіси «Перевірка за базою недійсних документів» (https://dmsu.gov.ua/services/nd.html) та «Єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань» (https://usr.minjust.gov.ua/content/government-agencies-request або (https://usr.minjust.gov.ua/content/home).

Ідентифікація фізичної особи здійснюється за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

Фізична особа може бути ідентифікована КНЕДП – АЦСК МВС за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті, за умови чинності цього сертифіката на момент звернення для отримання КЕД послуги.

Перелік документів, які повинен надати користувач:

1) Фізична особа:
- заява про реєстрацію;
- оригінал паспортного документа (для ознайомлення);
- копія паспортного документа;
- оригінал облікової картки платника податків (за наявності, для ознайомлення);
- копія облікової картки платника податків (за наявності);

2) Юридична особа, уповноважений представник юридичної особи:
- заява про реєстрацію;
- оригінал паспортного документа (для ознайомлення);
- копія паспортного документа;
- оригінал облікової картки платника податків (за наявності, для ознайомлення);
- копія облікової картки платника податків (за наявності);

- копія наказу (витяг з наказу) про призначення на посаду в юридичній особі (для керівника юридичної особи - обов'язково, іншим представникам юридичної особи - за необхідності внесення до кваліфікованого сертифіката відомостей про посаду уповноваженого представника юридичної особи);
- оригінал установчого документа/його засвідчена копія (для ознайомлення);
- витяг з ЄДР;
- копія наказу, довіреності, іншого документа, оформленого на ім'я уповноваженого представника юридичної особи, що підтверджує його повноваження на укладення правочинів з третіми особами (у разі відсутності відповідної інформації про уповноваженого представника юридичної особи в ЄДР).

3) Державна установа, уповноважений представник державної установи:

- документи, передбачені для юридичної особи, уповноваженого представника юридичної особи;копія наказу про визначення відповідального підрозділу (відповідального працівника) за організацію використання кваліфікованих електронних довірчих послуг у державній установі;
- копія наказу про уповноважених працівників державної установи, відповідальних за використання кваліфікованої електронної печатки.

4) Самозайнята особа (нотаріус, адвокат, арбітражний керуючий, приватний виконавець тощо):

- заява про реєстрацію;
- оригінал паспортного документа (для ознайомлення);
- копія паспортного документа;
- оригінал облікової картки платника податків (за наявності, для ознайомлення);
- копія облікової картки платника податків (за наявності);

5) Фізична особа-нерезидент:

- заява про реєстрацію;
- оригінал посвідки на постійне (тимчасове) місце проживання, паспортного документа громадянина іншої країни (посвідчення біженця) (для ознайомлення) з нотаріально засвідченим перекладом українською мовою;
- копія посвідки на постійне (тимчасове) місце проживання, паспортного документа громадянина іншої країни (посвідчення біженця) із нотаріально засвідченим перекладом українською мовою;
- оригінал облікової картки платника податків (за наявності, для ознайомлення); - копія облікової картки платника податків (за наявності);

6) Представництво юридичної особи - нерезидента, уповноважений представник юридичної особи - нерезидента:

- заява про реєстрацію;
- оригінал паспортного документа (для ознайомлення);
- копія паспортного документа;
- оригінал облікової картки платника податків (за наявності, для ознайомлення);
- копія облікової картки платника податків (за наявності);
- копія наказу про призначення на посаду в юридичній особі - нерезиденті (за необхідності внесення до кваліфікованого сертифіката відомостей про посаду уповноваженого представника юридичної особи - нерезидента);
- оригінал свідоцтва про реєстрацію (для ознайомлення) та його завірена копія, виданого Міністерством економіки України або Міністерством фінансів України;
- витяг з ЄДР;
- засвідчена копія довіреності, договору з керівником (керуючим) представництва юридичної особи - нерезидента;

7) Юридична особа - нерезидент, уповноважений представник юридичної особи - нерезидент:

- заява про реєстрацію;
- оригінал паспортного документа (для ознайомлення);
- копія паспортного документа;
- оригінал облікової картки платника податків (за наявності, для ознайомлення);
- копія облікової картки платника податків (за наявності);
- копія документа про призначення на посаду в юридичній особі - нерезиденті (за необхідності внесення до кваліфікованого сертифіката відомостей про посаду уповноваженого представника юридичної особи - нерезидента);
- витяг з ЄДР(за наявності);
- копія документа про реєстрацію (код/номер з торговельного, банківського чи судового реєстру, що ведеться країною резидентства іноземної юридичної особи, код/номер з реєстраційного посвідчення місцевого органу влади іноземної держави про реєстрацію юридичної особи), крім 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.

4.2. Обробка запиту на формування сертифіката

Запитом на формування кваліфікованого сертифіката є файл формату PKCS#10, що містить відкритий ключ користувача і додаткову інформацію для формування кваліфікованого сертифіката, який формується під час генерації особистого та відкритого ключів користувача засобами КЕП.

Запит на формування кваліфікованого сертифіката подається до КНЕДП – АЦСК МВС в особі адміністратора реєстрації (віддаленого адміністратора реєстрації, уповноваженого працівника ДМС) разом із заявою про реєстрацію від осіб, зазначених у пункті 4.1 цих Положень сертифікаційних практик, на знімному носієві інформації (USB-Flash накопичувач).

У випадку здійснення процедури подачі запиту на формування кваліфікованого сертифіката для користувачів, які мають чинний кваліфікований сертифікат, сформований КНЕДП – АЦСК МВС, запит на формування кваліфікованого сертифіката подається автоматично після генерації нових пар ключів із застосуванням он-лайн сервісу КНЕДП – АЦСК МВС (який є складовою частиною програмно-технічного комплексу формування кваліфікованого сертифіката) та з використанням засобів криптографічного захисту інформації.

Обробка запиту на формування кваліфікованого сертифіката здійснюється програмними засобами ІКС КНЕДП – АЦСК МВС уповноваженим працівником 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 на формування кваліфікованого сертифіката включає процеси 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 КНЕДП – АЦСК МВС та забезпечується унікальність серійного номера кваліфікованого сертифіката користувача у КНЕДП – АЦСК МВС.

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

4.3. Видача сертифіката

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

- шляхом публікації сформованого кваліфікованого сертифіката на офіційному веб-сайті КНЕДП – АЦСК МВС (за умови надання згоди користувачем);
- шляхом запису файлу із сформованим кваліфікованим сертифікатом ключа на знімний носій інформації (USB-Flash накопичувач), наданий користувачем (на вимогу користувача);
- шляхом надсилання файлу із сформованим кваліфікованим сертифікатом ключа на адресу електронної пошти, вказану в заяві про реєстрацію (на вимогу користувача);
- шляхом надання інформації про кваліфікований сертифікат ключа в роздрукованому вигляді (на вимогу користувача).

4.4. Прийняття сертифіката

Користувач повинен протягом доби перевірити свої ідентифікаційні дані, внесені до кваліфікованого сертифіката КНЕДП – АЦСК МВС. КНЕДП –АЦСК МВС повинен надавати відповідні консультації щодо проведення такої перевірки.

Користувач повинен використовувати особистий ключ тільки за результатом його успішної перевірки. Використання користувачем особистого ключа є фактом визнання ним правильності даних внесених до кваліфікованого сертифіката відповідного відкритого ключа.

У разі невідповідності ідентифікаційних даних, внесених КНЕДП – АЦСК МВС до кваліфікованого сертифіката та виявлених користувачем після отримання сформованого кваліфікованого сертифіката, власник такого сертифіката (уповноважений представник створювача електронної печатки) особисто звертається до КНЕДП – АЦСК МВС для скасування цього сертифіката та формування нового кваліфікованого сертифіката у порядку, встановленому п. 4.7 Положень сертифікаційних практик.

4.5. Пара ключів та призначення сертифіката

4.5.1. Використання особистого ключа та сертифіката користувачем

Користувач повинен використовувати особистий ключ та кваліфікований сертифікат згідно з вимогами законодавства у сферах електронної ідентифікації та електронних довірчих послуг та відповідно до:

- Регламенту, Практики сертифіката, Положень сертифікаційних практик;
- Договору про надання кваліфікованих електронних довірчих послуг (договір приєднання), укладеного з МВС.

Для отримання кваліфікованого сертифіката користувач повинен:

- ознайомитись з Регламентом, Практикою сертифіката, Положеннями сертифікаційних практик (https://ca.mvs.gov.ua/reglament) та Договором про надання КЕД послуг (https://ca.mvs.gov.ua/user-downloads).
- підготувати необхідні для отримання КЕД послуг документи та заяви;
- звернутися із підготовленими заявами, пакетом документів та засобом КЕП до КНЕДП – АЦСК МВС або ВПР КНЕДП – АЦСК МВС;

- пройти процедуру первинної ідентифікації та надати підготовлені для реєстрації документи, заяви;

з допомогою працівника КНЕДП – АЦСК МВС або ВПР КНЕДП – АЦСК МВС здійснити генерацію особистого ключа та відповідного йому відкритого ключа у засобі КЕП. У випадку, коли генерацію ключа здійснено самостійно з використанням програмного комплексу «Користувач АЦСК МВС України» поза межами КНЕДП – АЦСК МВС або ВПР КНЕДП – АЦСК МВС, надати збережений на USB Flash накопичувачі запит формату PKCS#10 для формування кваліфікованих сертифікатів працівнку КНЕДП – АЦСК МВС або ВПР КНЕДП – АЦСК МВС.

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

Під час використання відкритого ключа та кваліфікованого сертифіката користувача суб'єктами, які довіряють КНЕДП – АЦСК МВС, повинні дотримуватися вимог законодавства у сфері електронних довірчих послуг, а також положень:

- Регламенту, Політики сертифіката та цих Положень сертифікаційних практик.

Пункт 4.5.2 Політики сертифіката містить додаткову інформацію щодо використання відкритого ключа та кваліфікованого сертифіката суб'єктами, які довіряють КНЕДП – АЦСК МВС.

4.6. Поновлення сертифіката

КНЕДП – АЦСК МВС не пізніше ніж протягом двох годин поновлює заблокований кваліфікований сертифікат, у разі:

- подання користувачем заяви про поновлення його заблокованого кваліфікованого сертифіката;

- подання заяви про поновлення кваліфікованого сертифіката працівника юридичної особи за підписом уповноваженої особи відповідної юридичної особи;

- повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа користувачем або контролюючим органом, який раніше повідомив про таку підозру;

- надходження до КНЕДП – АЦСК МВС повідомлення про прийняття рішення суду про поновлення кваліфікованого сертифіката, що набрало законної сили.

Заява щодо поновлення кваліфікованого сертифіката подається до КНЕДП – АЦСК МВС користувачами за формою, яка публікується на офіційному веб-сайті КНЕДП – АЦСК МВС.

КНЕДП – АЦСК МВС повинен встановити (ідентифікувати) особу, яка звертається із заявою щодо поновлення кваліфікованого сертифіката, а також перевірити законність такого звернення.

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

Перелік документів та рекомендації щодо їх оформлення публікуються на офіційному веб-сайті КНЕДП – АЦСК МВС.

Максимальний час між отриманням заяви щодо поновлення кваліфікованого сертифіката та зміною його статусу не повинен перевищувати двох годин.

Інформація про зміну статусу кваліфікованого сертифіката на «чинний» розповсюджується шляхом формування та публікації КНЕДП – АЦСК МВС списків відкликаних сертифікатів та за протоколом інтерактивного визначення статусу сертифіката (OCSP), що публікуються на офіційному веб-сайті КНЕДП – АЦСК МВС.

4.7. Повторне формування сертифіката

Повторне формування кваліфікованих сертифікатів здійснюється у разі виявлення невідповідності ідентифікаційних даних, внесених КНЕДП – АЦСК МВС до кваліфікованих сертифікатів та виявлених працівником КНЕДП – АЦСК МВС або користувачем.

На підставі наданих користувачем заяв та документів, що підтверджують зміни відомостей, що містяться у кваліфікованих сертифікатах, КНЕДП – АЦСК МВС здійснює повторне формування кваліфікованих сертифікатів та їх публікації в разі згоди користувача.

Повторне формування кваліфікованого сертифіката здійснюється працівником КНЕДП – АЦСК МВС із використанням попередньо засвідченого відкритого ключа користувача. Повторне формування кваліфікованого сертифіката не продовжує строку його дії.

Працівник КНЕДП – АЦСК МВС, який ініціював повторне формування кваліфікованого сертифіката, складає акт, в якому зазначається дата та час скасування кваліфікованого сертифіката, ідентифікаційні дані користувача, що містяться у кваліфікованому сертифікаті та невідповідні ідентифікаційні дані користувача, що зазначені у заяві про реєстрацію. Акт підписується посадовою особою КНЕДП – АЦСК МВС, що ініціювала повторне формування кваліфікованого сертифіката, та адміністратором сертифікації, після цього долучається до особової справи КНЕДП – АЦСК МВС.

4.8. Зміна сертифіката

Зміна ідентифікаційних даних, що внесені до кваліфікованого сертифіката користувача, є підставою для скасування кваліфікованого сертифіката та, у випадку необхідності, формування нових кваліфікованих сертифікатів після внесення таких змін на підставі наданих користувачем відповідних заяв та документів.

4.9. Блокування та скасування сертифіката

4.9.1. Обставини для скасування кваліфікованого сертифіката

Скасування кваліфікованого сертифіката здійснюється КНЕДП – АЦСК МВС у разі:

1) подання до КНЕДП – АЦСК МВС заяви про скасування/ запиту на скасування;

2) надходження до КНЕДП – АЦСК МВС документа, що підтверджує:

- державну реєстрацію припинення юридичної особи або припинення підприємницької діяльності фізичної особи - підприємця, яка є створювачем електронної печатки;

- смерть фізичної особи, яка є підписувачем, або фізичної особи - підприємця, яка є створювачем електронної печатки;

- зміну ідентифікаційних даних користувача, які містяться у кваліфікованому сертифікаті;

- надання користувачем недостовірних ідентифікаційних даних під час формування його кваліфікованого сертифіката;

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

- набрання законної сили рішенням суду про скасування кваліфікованого сертифіката відкритого ключа, оголошення фізичної особи, яка є підписувачем, або фізичної особи - підприємця, яка є створювачем електронної печатки, померлою, визнання її безвісно відсутньою, недієздатною, обмеження її цивільної дієздатності, визнання користувача електронних довірчих послуг банкрутом.

4.9.2. Особи, які можуть подавати заяви на скасування

КНЕДП – АЦСК МВС скасовує сформований ним кваліфікований сертифікат у разі:

- подання користувачем заяви на скасування виданого йому кваліфікованого сертифіката в будь-який спосіб, що забезпечує підтвердження особи користувача;

- подання заяви на скасування кваліфікованого сертифіката працівника юридичної особи чи фізичної особи - підприємця за підписом уповноваженої особи відповідної юридичної особи чи фізичної особи - підприємця;

- подання заяви на скасування сертифіката ключа колишнього працівника відповідальним підрозділом (працівником) юридичної особи чи фізичної особи - підприємця;

- отримання від ДМС запиту на скасування кваліфікованого сертифіката користувача, на ім'я якого оформлено паспорт громадянина України з імплантованим БЕН та який отримав у КНЕДП – АЦСК МВС КЕД послуги у зв'язку з генерацією на БЕН першої пари ключів (скасування кваліфікованого сертифіката здійснюється відповідно до законодавства України);

- у разі настання інших умов, передбачених статтею 25 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», відповідальний підрозділ (працівник) може надати КНЕДП – АЦСК МВС за підписом уповноваженої особи відповідної державної установи заяву про скасування кваліфікованого сертифіката відкритого ключа підписувача - представника державної установи, що використовувався таким підписувачем - представником державної установи.

4.9.3. Процедура запиту на скасування

КНЕДП – АЦСК МВС повинен ідентифікувати особу, яка звертається із заявою на скасування сертифіката, а також перевірити законність такого звернення.

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

Ідентифікація КНЕДП – АЦСК МВС користувача також може здійснюватися за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті, за умови чинності цього сертифіката.

Заява на скасування кваліфікованого сертифіката в електронному вигляді формується користувачем за допомогою засобів КЕП, які надаються КНЕДП – АЦСК МВС (за технічної можливості), та передається до ІКС КНЕДП – АЦСК МВС у вигляді електронного документа, зокрема HTTP-запиту. При цьому, заява щодо скасування кваліфікованого сертифіката в електронному вигляді засвідчується власним КЕП користувача з використанням чинного кваліфікованого сертифіката, сформованого КНЕДП – АЦСК МВС.

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

Перелік документів, необхідних для подання заяви на скасування кваліфікованого сертифіката, та рекомендації щодо їх оформлення публікуються на офіційному веб-сайті КНЕДП – АЦСК МВС.

Кваліфікований сертифікат втрачає чинність з моменту зміни КНЕДП – АЦСК МВС статусу кваліфікованого сертифіката на «скасований».

Скасований кваліфікований сертифікат поновленню не підлягає.

Інформація про зміну статусу кваліфікованого сертифіката на «скасований» розповсюджується шляхом формування та публікації КНЕДП – АЦСК МВС списків відкликаних сертифікатів та за протоколом інтерактивного визначення статусу сертифіката (OCSP).

4.9.4. Блокування кваліфікованого сертифіката

КНЕДП – АЦСК МВС блокує сформований ним кваліфікований сертифікат протягом двох годин у разі:

- подання заяви користувачем на блокування виданого йому кваліфікованого сертифіката в будь-який спосіб, що забезпечує підтвердження його особи;

- набрання законної сили рішенням суду про блокування кваліфікованого сертифіката відкритого ключа та надходження до КНЕДП – АЦСК МВС такого рішення;

- подання заяви про блокування кваліфікованого сертифіката відкритого ключа електронного підпису працівника юридичної особи чи фізичної особи - підприємця за підписом уповноваженої особи відповідної юридичної особи чи фізичної особи - підприємця;

- повідомлення користувачем або контролюючим органом про підозру в компрометації особистого ключа користувача;

- порушення користувачем електронних довірчих послуг істотних умов договору про надання кваліфікованих електронних довірчих послуг;

- у разі прийняття контролюючим органом рішення про блокування відповідного кваліфікованого сертифіката відкритого ключа за результатами здійснення заходів державного контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг відповідно до Закону.

Заява щодо блокування кваліфікованого сертифіката подається до КНЕДП – АЦСК МВС:

- письмово користувачем (форма заяви публікується на офіційному веб-сайті КНЕДП – АЦСК МВС);в електронній формі шляхом формування користувачем запиту на блокування сертифіката ключа із використанням особистого ключа, засобу КЕП, наданого КНЕДП – АЦСК МВС, та чинного кваліфікованого сертифіката користувача, сформованого КНЕДП – АЦСК МВС ;

- усно із проходженням процедури голосової автентифікації за ключовою фразою, обумовленою під час реєстрації користувача.

У випадку тимчасового вилучення паспорта громадянина України з імплантованим БЕН чинні кваліфіковані сертифікати фізичної особи, на ім’я якої оформлено паспорт, блокуються

КНЕДП – АЦСК МВС шляхом подачі користувачем у встановленому порядку заяви щодо блокування кваліфікованих сертифікатів ключів.

З метою забезпечення захисту особистого ключа від компрометації користувач, на ім'я якого оформлено тимчасово вилучений паспорт громадянина України з імплантованим БЕН, зобов'язаний не розголошувати та не повідомляти особам, якими вилучено паспорт, пароль доступу до особистого ключа (значення ПІН1(2) та ПАК1(2)) та ключову фразу для голосової автентифікації.

Після блокування кваліфікованого сертифіката користувач може протягом тридцяти календарних днів поновити чинність кваліфікованого сертифіката. Блокований кваліфікований сертифікат буде автоматично скасований КНЕДП – АЦСК МВС, якщо протягом зазначеного строку користувач не поновить його чинність.

КНЕДП – АЦСК МВС повинен встановити (ідентифікувати) особу, яка звертається із заявою щодо блокування кваліфікованого сертифіката, а також перевірити законність такого звернення.

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

Встановлення фізичної особи КНЕДП – АЦСК МВС також здійснюється за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті, за умови чинності цього сертифіката.

Форма письмової заяви на блокування, перелік необхідних документів та рекомендації щодо їх оформлення публікуються на офіційному веб-сайті КНЕДП – АЦСК МВС.

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

Заява щодо блокування кваліфікованого сертифіката в електронному вигляді формується користувачем за допомогою засобів КЕП, які надаються КНЕДП – АЦСК МВС (за технічної можливості), та передається до ІКС КНЕДП – АЦСК МВС у вигляді електронного документа, зокрема HTTP-запиту. При цьому, заява щодо блокування кваліфікованого сертифіката в електронному вигляді засвідчується власним КЕП користувача з використанням чинного кваліфікованого сертифіката, сформованого КНЕДП – АЦСК МВС.

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

За результатами обробки усної заяви щодо блокування кваліфікованого сертифіката, посадова особа КНЕДП – АЦСК МВС, що прийняла заяву, складає акт, в якому зазначається дата та час подання заяви, ідентифікаційні дані користувача, створювача електронної печатки що містяться у кваліфікованому сертифікаті та ключова фраза, обумовлена під час реєстрації користувача, створювача електронної печатки. Акт підписується двома посадовими особами

КНЕДП – АЦСК МВС та долучається до особової справи користувача, створювача електронної печатки.

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

Інформація про зміну статусу кваліфікованого сертифіката на «блокований» розповсюджується шляхом формування та публікації КНЕДП – АЦСК МВС списків відкликаних сертифікатів та за протоколом інтерактивного визначення статусу сертифіката (OCSP).

Кваліфікований сертифікат відкритого ключа вважається заблокованим з моменту зміни КНЕДП – АЦСК МВС, статусу кваліфікованого сертифіката відкритого ключа на «заблокований».

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

Блокований кваліфікованого сертифікат може бути поновлений за умов, визначених у цьому Регламенті.

Перелік підстав для зміни статусу кваліфікованого сертифіката на “блокований” та “скасований” із зазначенням суб’єктів подання запитів на зміну статусу та форм підтвердження підстав наведений у Таблиці 7.

Таблиця 7. Перелік підстав для зміни статусу кваліфікованого сертифіката на «блокований» та «скасований»

Підстави для зміни статусу сертифіката	**Скасування**	**Блокування**	**Підтвердження підстав**
Подання користувачем заяви	+	+	Заява користувача
Смерть фізичної особи - користувача	+		Документальне підтвердження
Припинення діяльності створювача електронної печатки (юридичної особи або фізичної особи - підприємця)	+		Документальне підтвердження
Зміни ідентифікаційних даних користувача	+		Документальне підтвердження
Надання користувачем недостовірних ідентифікаційних даних	+		Документальне підтвердження

Факт компрометації особистого ключа користувача, виявлений самостійно користувачем або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері КЕД послуг	+		Документальне підтвердження або заява користувача
Повідомлення користувачем або контролюючим органом про підозру в компрометації особистого ключа користувача КЕД послуг		+	Заява користувача або документальне підтвердження
Набрання законної сили рішенням суду	+	+	Документальне підтвердження
Порушення користувачем істотних умов договору про надання КЕД послуг		+	Документальне підтвердження

Перелік та опис механізмів автентифікації користувачів з питань блокування або скасування кваліфікованого сертифіката наведено у Таблиці 6 цих Положень сертифікаційних практик.

Кваліфіковані сертифікати скасовується та блокуються КНЕДП – АЦСК МВС не пізніше ніж протягом двох годин від моменту отримання підтвердження підстав для зміни статусу кваліфікованого сертифіката та здійснення відповідної перевірки достовірності документальних повідомлень та автентифікації користувачів.

4.10. Послуга перевірки 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.

Користувач може звернутися до КНЕДП – АЦСК МВС із заявою про скасування виданого йому кваліфікованого сертифіката у разі необхідності дострокового припинення його обслуговування за процедурою визначеною в пункті 4.9 цих Положень сертифікаційних практик.

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

4.12. Депонування та відновлення ключа

Не застосовується.

5. ОБ'ЄКТ, УПРАВЛІННЯ ТА ОПЕРАЦІЙНИЙ КОНТРОЛЬ

До об'єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.4 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

5.1. Контроль фізичної безпеки

Пункт 5.1 Політики сертифіката містить інформацію щодо вимог до приміщень КНЕДП – АЦСК МВС та забезпечення фізичного доступу до них.

5.2. Процедурний контроль

Пункт 5.3 Політики сертифіката містить інформацію щодо довірених ролей персоналу КНЕДП – АЦСК МВС (керівник, адміністратор реєстрації, адміністратор сертифікації, адміністратор безпеки, системний адміністратор, аудитор системи) та їх функціональних обов'язків, щодо кількості осіб, необхідних для виконання завдань, а також довірених ролей персоналу КНЕДП – АЦСК МВС, що вимагають розподілу обов'язків.

5.3. Контроль персоналу

Пункт 5.3 Політики сертифіката містить інформацію щодо вимог до кваліфікації, досвіду та допуску персоналу КНЕДП – АЦСК МВС вимог та процедур навчання, санкцій за несанкціоновані дії, моніторингу діяльності КНЕДП – АЦСК МВС відокремлених пунктів реєстрації КНЕДП – АЦСК МВС документації, яка надається персоналу КНЕДП – АЦСК МВС.

5.4. Ведення журналу аудиту подій

Пункти 5.3.7-5.3.13 Політики сертифіката містять інформацію щодо типів записаних подій, частоти обробки журналу аудиту подій, строків зберігання журналу аудиту подій, захисту журналу аудиту подій, процедур резервного копіювання журналу аудиту подій та питань синхронізації часу.

5.5. Архів документів

Пункт 5.4 Політики сертифіката (містить інформацію щодо видів документів та даних, що підлягають архівному зберіганню, строків зберігання архіву, захисту архіву, процедур резервного копіювання архіву, вимог щодо накладання електронних позначок часу на записи, систем збирання архівів, процедур отримання та перевірки архівної інформації.

5.6. Зміна ключа

Пункт 5.5 Політики сертифіката містить інформацію щодо підстав та періодичності зміни пари ключів КНЕДП – АЦСК МВС порядку використання та доступу до актуального відкритого ключа КНЕДП – АЦСК МВС.

5.7. Компрометація і аварійне відновлення

Пункт 5.6 Політики сертифіката містить інформацію щодо процедур обробки інцидентів і компрометації, процедур відновлення, якщо обчислювальні ресурси, програмне забезпечення та/або дані пошкоджені, процедур відновлення після компрометації особистого ключа, можливостей безперервності бізнесу після катастрофи.

5.8. Припинення діяльності КНЕДП – АЦСК МВС

Пункт 5.7 Політики сертифіката містить інформацію щодо підстав припинення діяльності КНЕДП – АЦСК МВС, порядку надання повідомлення про припинення діяльності, визначення дати припинення діяльності, питань правонаступництва та передачі документованої інформації, а також Плану припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП – АЦСК МВС.

6. ТЕХНІЧНІ ЗАХОДИ БЕЗПЕКИ

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.5 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

6.1. Генерація та встановлення пари ключів

Пункт 6.1 Політики сертифіката містить інформацію щодо генерації пари ключів КНЕДП – АЦСК МВС та користувачів, доставки особистого та відкритого ключів користувачам, доставки відкритого ключа КНЕДП – АЦСК МВС суб’єктами, які довіряють КНЕДП – АЦСК МВС, щодо розмірів ключів, генерації параметрів відкритого ключа КНЕДП – АЦСК МВС та перевірки якості, основних цілей використання особистих ключів КНЕДП – АЦСК МВС.

6.2. Захист особистого ключа та інженерний контроль криптографічного модуля

Пункт 6.2 Політики сертифіката містить інформацію щодо стандартів та елементів керування криптографічним модулем, резервного копіювання особистого ключа, архівації особистого ключа, відновлення особистого ключа, зберігання особистого ключа в криптографічному модулі, активації особистих ключів, деактивації особистих ключів, знищення особистих ключів, можливостей мережного криптографічного модуля.

6.3. Інші аспекти керування парами ключів

Пункт 6.3 Політики сертифіката містить інформацію щодо архівації відкритого ключа КНЕДП – АЦСК МВС строків дії сертифіката та строків використання пари ключів КНЕДП – АЦСК МВС

6.4. Дані активації

Пункт 6.4 Політики сертифіката містить інформацію щодо захисту даних активації особистого ключа.

6.5. Контроль комп'ютерної безпеки

Пункт 6.5 Політики сертифіката містить інформацію щодо спеціальних технічних вимог до комп’ютерної безпеки, рейтингу комп’ютерної безпеки.

6.6. Контроль безпеки життєвого циклу

Пункт 6.6 Політики сертифіката містить інформацію щодо контролю розробки ІКС КНЕДП – АЦСК МВС, засобів керування безпекою в ІКС КНЕДП – АЦСК МВС контролю безпеки протягом життєвого циклу.

6.7. Контроль безпеки мережі

Пункт 6.7 Політики сертифіката містить інформацію щодо елементів керування безпекою мережі.

6.8. Електронні позначки часу

Пункт 6.8 Політики сертифіката містить інформацію щодо формування та перевірки кваліфікованої електронної позначки часу, наслідків недійсності кваліфікованої електронної

позначки часу та процедури отримання КНЕДП – АЦСК МВС кваліфікованої електронної позначки часу.

7. ПРОФІЛІ СЕРТИФІКАТІВ, СПИСКІВ ВІДКЛИКАНИХ СЕРТИФІКАТІВ (CRL) ТА ПРОТОКОЛА 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

Пункт 7.1 Політики сертифіката містить інформацію щодо відомостей, які повинні міститися в кваліфікованих сертифікатах.

7.2. Профілі списку відкликаних сертифікатів

Пункт 7.2 Політики сертифіката містить інформацію щодо відомостей, які повинні міститися в списках відкликаних сертифікатів.

7.3. Профілі протоколу визначення статусу сертифіката

Пункт 7.3 Політики сертифіката містить інформацію щодо можливості перевірки статусу кваліфікованого сертифіката користувача в режимі реального часу через електронні комунікаційні мережі загального користування із використанням протоколу 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

Пункт 8.1 Політики сертифіката містить інформацію щодо частоти та обставин оцінювання КНЕДП – АЦСК МВС.

8.2. Особа/кваліфікація оцінювача

Пункт 8.2 Політики сертифіката містить інформацію щодо вимог до кваліфікації посадових осіб КО та ООВ.

8.3. Відносини експерта з об’єктом оцінки

Пункт 8.3 Політики сертифіката містить інформацію щодо відносин посадових осіб КО та експертів (аудиторів) органу з оцінки відповідності з об'єктом оцінки КНЕДП – АЦСК МВС.

8.4. Теми, охоплені оцінюванням

Пункт 8.4 Політики сертифіката містить інформацію щодо питань, які підлягають перевірці під час державного контролю та під час оцінки відповідності.

8.5. Дії, вжиті внаслідок порушення

Пункт 8.5 Політики сертифіката містить інформацію щодо дій, які вживаються внаслідок порушення, виявленого за результатами державного контролю або за результатами оцінки відповідності.

8.6. Повідомлення результатів

Пункт 8.6 Політики сертифіката містить інформацію щодо оформлення результатів державного контролю або оцінки відповідності, надання припису про усунення порушень, виявлених під час державного контролю.

8.7. Самоперевірки

Пункт 8.7 Політики сертифіката містить інформацію щодо проведення КНЕДП – АЦСК МВС регулярних внутрішніх аудитів дотримання встановлених вимог.

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 довірчі послуги, що надаються КНЕДП – АЦСК МВС

Всі кваліфіковані електронні довірчі послуги, що надаються КНЕДП – АЦСК МВС та ВПР КНЕДП – АЦСК МВС, безоплатні.

9.2. Фінансова відповідальність

Пункт 9.2 Політики сертифіката містить інформацію щодо фінансової відповідальності КНЕДП – АЦСК МВС.

9.3. Конфіденційність особистої інформації

Пункт 9.3 Політики сертифіката містить інформацію щодо змісту та обсягу конфіденційної інформації, що знаходиться в розпорядженні КНЕДП – АЦСК МВС а також відповідальності за захист конфіденційної інформації.

9.4. Захист персональних даних

Пункт 9.4 Політики сертифіката містить інформацію щодо концепції захисту персональних даних в КНЕДП – АЦСК МВС визначення персональних даних, а також персональних даних, що не вважаються конфіденційними, щодо відповідальності за захист персональних даних, щодо згоди на використання персональних даних та обставин розкриття персональних даних.

9.5. Права інтелектуальної власності

Питання прав інтелектуальної власності КНЕДП – АЦСК МВС врегульовані відповідно до вимог чинного законодавства України.

9.6. Заяви та гарантії

Пункт 9.6 Політики сертифіката містить інформацію щодо зобов'язань та гарантій КНЕДП – АЦСК МВС, відокремлених пунктів реєстрації КНЕДП – АЦСК МВС, користувачів, довіряючих сторін, а також інших учасників.

9.7. Відмова від відповідальності

Пункт 9.7 Політики сертифіката містить інформацію щодо відмови від гарантій КНЕДП – АЦСК МВС.

9.8. Обмеження відповідальності

Пункт 9.8 Політики сертифіката містить інформацію щодо обставин для обмеження відповідальності КНЕДП – АЦСК МВС.

9.9. Відшкодування

Пункт 9.9 Політики сертифіката містить інформацію щодо відшкодування шкоди, яка може бути завдана користувачам КЕД послуг чи третім особам внаслідок неналежного виконання КНЕДП – АЦСК МВС.

9.10. Термін дії та припинення дії

Положення сертифікаційних практик застосовуються з моменту його публікації та діють до закінчення строку дії останнього сертифіката, виданого відповідно до Регламента або до моменту припинення діяльності КНЕДП – АЦСК МВС.

9.11. Індивідуальні комунікації з суб'єктами 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;
- надсилання електронних листів на адресу електронної пошти користувача;
- здійснення телефонних дзвінків на номер телефона користувача.

9.12. Зміни

Внесення змін та доповнень до цих Положень сертифікаційних практик здійснюється КНЕДП – АЦСК МВС у випадку:

- змін у законодавстві;
- змін вимог, процесів та процедур, описаних у Регламенті, Політиці сертифіката та цих Положеннях сертифікаційних практик;
- змін у вимогах до КНЕДП – АЦСК МВС щодо надання послуг.

Нові версії цих Положень сертифікаційних практик після внесення змін до них, публікуються на веб-сайті КНЕДП – АЦСК МВС.

Будь-які зміни, не зазначені в історії цих Положень сертифікаційних практик, є граматичними і орфографічними змінами, які не впливають на суть та не стосуються процесів та процедур описаних в цих Положеннях сертифікаційних практик.

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 цими Положеннями сертифікаційних практик, поширюється чинне законодавство України.

9.15. Дотримання чинного законодавства

Пункт 9.15 Політики сертифіката КНЕДП – АЦСК МВС містить інформацію щодо нормативно - правових актів, які встановлюють вимоги до надання КНЕДП – АЦСК МВС кваліфікованих електронних довірчих послуг.