Додаток 1

до Регламенту роботи Кваліфікованого надавача електронних довірчих послуг «MASTERKEY» ТОВ «АРТ-МАСТЕР»

ПОЛІТИКА СЕРТИФІКАТА

Кваліфікованого надавача електронних довірчих послуг «MASTERKEY»

ЗМІСТ

1. ВСТУП

1.1. Огляд

Ця Політика сертифіката визначає перелік усіх правил, що застосовуються кваліфікованим надавачем електронних довірчих послуг «MASTERKEY» (далі - Надавач) у процесі реєстрації користувачів електронних довірчих послуг, зокрема, підписувачів та створювачів електронних печаток (далі - користувачі) формування та обслуговування кваліфікованих сертифікатів відкритих ключів (далі - кваліфіковані сертифікати) Надавача та користувачів, зокрема, управління їх статусом (блокування, поновлення та скасування).

Дотримання вимог, визначених у цій Політиці сертифіката, є обов'язковим для керівника підрозділу Надавача та найманих працівників Надавача, посадові обов'язки яких безпосередньо пов'язані з реєстрацією користувачів, формуванням та обслуговуванню їхніх кваліфікованих сертифікатів (далі - персонал), а також юридичних та фізичних осіб-підприємців, які на підставі договорів укладених з ТОВ «АРТ-МАСТЕР» пов'язані з реєстрацією користувачів, зокрема, відокремлених пунктів реєстрації Надавача.

Визнання користувачами вимог, визначених у цій Політиці сертифіката, є обов'язковою умовою та підставою для укладення з ними договору про надання електронних довірчих послуг.

Перелік усіх практичних дій та процедур, які застосовуються для реалізації Надавачем цієї Політики сертифіката, визначають:

- Положення сертифікаційних практик КНЕДП «MASTERKEY» щодо кваліфікованих сертифікатів електронного підпису та печатки.

Ця Політика сертифіката відповідає вимогам, визначеним у стандартах:

- 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 319 401 (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

Повна назва документа: Політика сертифіката Кваліфікованого Надавача електронних довірчих послуг «MASTERKEY»

Скорочена назва документа: Політика сертифіката КНЕДП «MASTERKEY»

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

1.3. Учасники інфраструктури відкритих ключів

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

1.3.1. Надавач

КНЕДП «MASTERKEY» є кваліфікованим надавачем електронних довірчих послуг, що надає кваліфіковані електронні довірчі послуги з дотриманням вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги», зокрема, здійснює реєстрацію користувачів самостійно або через відокремлені пункти реєстрації Надавача, формує та обслуговує їхні кваліфіковані сертифікати в тому числі здійснює управління їхнім статусом (блокування, поновлення та скасування).

1.3.1.1. Права Надавача

Надавач має право:
- надавати електронні довірчі послуги з дотриманням вимог законодавства у сфері електронних довірчих послуг;
- отримувати документи, 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 публічних електронних реєстрів відповідно до Закону України «Про публічні електронні реєстри»;
- звертатися до ЦЗО із заявами про формування кваліфікованих сертифікатів, їх скасування, блокування або поновлення.

1.3.1.2. Обов'язки Надавача

Надавач зобов'язаний забезпечувати:
- захист персональних даних Користувачів відповідно до вимог Закону України «Про захист персональних даних»;
- функціонування інформаційно-комунікаційної системи та програмно-технічного комплексу, що використовуються для надання електронних довірчих 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-сайту 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;

- цілодобовий прийом та перевірку заяв в електронній формі підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів. Прийом та перевірку заяв у паперовій формі підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів протягом робочого дня згідно з режимом роботи надавача електронних довірчих послуг та його відокремлених пунктів реєстрації;
- скасування, блокування та поновлення кваліфікованих сертифікатів відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги»;
- встановлення під час формування сертифіката відкритого ключа належності відкритого ключа та відповідного йому особистого ключа підписувачу чи створювачу електронної печатки;
- внесення даних підписувача чи створювача електронної печатки до відповідного сертифіката відкритого ключа;
- вжиття організаційних і технічних заходів з управління ризиками, пов’язаними з безпекою електронних довірчих 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 електронних довірчих послуг або стосуються персональних даних користувачів електронних довірчих послуг, без необґрунтованої затримки, не пізніше ніж протягом 24 годин з моменту, коли їм стало відомо про таке порушення;
- інформування користувачів електронних довірчих послуг 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 їм 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 Надавача у межах надання послуги створення, перевірки та підтвердження електронного підпису чи електронної печатки;
- постійне зберігання всіх виданих сертифікатів відкритих ключів;
- постійне зберігання документів та електронних даних, отриманих у зв’язку з наданням електронних довірчих послуг;
- страхування відповідальності для забезпечення відшкодування шкоди, яка може бути завдана користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання кваліфікованим надавачем електронних довірчих послуг своїх зобов’язань;
- відновлення розміру страхової суми протягом трьох місяців у разі зміни розміру мінімальної заробітної плати або в разі відшкодування збитків, завданих користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання своїх зобов’язань;

- використання під час надання кваліфікованих електронних довірчих послуг виключно кваліфікованих сертифікатів відкритих ключів, сформованих центральним засвідчувальним органом;
- наймання працівників та, за потреби, виконання робіт субпідрядними організаціями, які володіють необхідними для надання електронних довірчих 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 електронної довірчої послуги, про умови використання такої послуги, у тому числі про будь-які обмеження її використання, перед укладенням договору про надання електронних довірчих послуг;
- інформування контролюючого органу та центрального засвідчувального органу або засвідчувального центру про намір припинити свою діяльність та про зміни у наданні кваліфікованих електронних довірчих послуг протягом 48 годин з моменту настання таких змін;
- передачу центральному засвідчувальному органу або іншому кваліфікованому надавачу електронних довірчих послуг документованої інформації в разі припинення діяльності з надання кваліфікованих електронних довірчих послуг;
- приєднання до програмного інтерфейсу ЦЗО з метою забезпечення інтероперабельності, дослідження поточного стану, перспектив розвитку сфери електронних довірчих послуг та виконання інших повноважень.

1.3.2. Органи реєстрації

Функції відокремлених пунктів реєстрації можуть виконувати як підрозділи або працівники Надавача (далі – ВПР Надавача) так і його Партнери - юридичні особи або ФОП, якими укладено з Надавачем відповідні договори, що містять спеціальні їх обов’язки та повноваження, в тому числі і вимоги щодо захисту інформації (далі – ВПР Надавача).

1.3.3. Користувачі

Користувачами є підписувачі та створювачі електронних печаток, з якими Надавач укладає договори на надання електронних довірчих послуг та здійснює їх реєстрацію самостійно або через відокремлені пункти реєстрації, з подальшим формуванням та обслуговуванням їхніх кваліфікованих сертифікатів.

1.3.3.1. Права Користувачів

Користувачі мають право:
- своєчасно отримувати електронні довірчі послуги;
- цілодобово користуватись вільним доступом до опублікованих кваліфікованих сертифікатів інших користувачів, до даних про статус

кваліфікованих сертифікатів, до реєстру кваліфікованих сертифікатів Надавача та до нормативних документів у сфері надання електронних довірчих послуг з використанням комунікаційних мереж загального користування;
- одержувати кваліфіковані сертифікати Надавача;
- одержувати списки відкликаних сертифікатів, сформовані Надавачем;
- застосовувати списки відкликаних сертифікатів, сформовані Надавачем, для перевірки статусу власних кваліфікованих сертифікатів та кваліфікованих сертифікатів інших користувачів;
- здійснювати ініціювання скасування, блокування або поновлення кваліфікованих сертифікатів відповідно до вимог Регламенту;
- оскаржувати дії чи бездіяльність Надавача у судовому порядку.

1.3.3.2. Обов'язки Користувачів

Користувачі зобов’язані:
- ознайомитись та дотримуватись умов надання електронних довірчих послуг, визначених відповідними нормативними документами;
- надавати під час реєстрації повну та достовірну інформацію, необхідну для його ідентифікації та формування кваліфікованих сертифікатів;
- зберігати у таємниці особистий ключ та вживати всіх можливих заходів для запобігання його втрати, розкриття, зміни назви, зміни формату чи несанкціонованого використання;
- не розголошувати ключову фразу голосової автентифікації;
- не розголошувати іншим особам пароль захисту захищеного носія особистого ключа, на якому знаходиться особистий ключ;
- використовувати особистий ключ виключно з метою, визначеною у кваліфікованому сертифікаті та додержуватися інших обмежень щодо сфери використання кваліфікованого сертифіката (за наявності);
- інформувати Надавача про події, що трапилися до закінчення строку чинності кваліфікованого сертифіката, зокрема: компрометацію особистого ключа, компрометацію паролю захисту захищеного носія особистого ключа, виявлені неточності або зміну даних, зазначених у кваліфікованому сертифікаті;
- не використовувати особистий ключ у разі його компрометації;
- не використовувати особистий ключ, відповідний до кваліфікованих сертифікатів, заява на скасування чи блокування яких подана до Надавача, протягом часу з моменту подання заяви і до моменту офіційного повідомлення про скасування кваліфікованих сертифікатів;
- своєчасно здійснювати оплату за електронні довірчі послуги передбачену договором про надання кваліфікованих електронних довірчих послуг, укладеним з Надавачем.

1.3.4. Суб’єкти, які довіряють Надавачу

Фізичні та юридичні особи, а також їхні інформаційно-комунікаційні системи є суб’єктами, які довіряють Надавачу, 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 обслуговуванням кваліфікованих сертифікатів Надавача та користувачів, є іншими учасниками.

До інших учасників належать також ЦЗО та КО, які є наглядовими органами щодо Надавача.

ЦЗО, зокрема:

- адміністратор інформаційно-комунікаційної системи ЦЗО формує кваліфіковані сертифікати Надавача з використанням самопідписаного сертифіката електронної печатки ЦЗО;
- погоджує цю Політику сертифіката та відповідні Положення сертифікаційних практик Надавача, зміни до них, а також направляє їх копії до КО;
- погоджує порядок синхронізації часу із Всесвітнім координованим часом (UTC) Надавача;
- погоджує План припинення діяльності Надавача.

КО (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 ООВ 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 КО перевірок Надавача;
- інформує громадськість у разі отримання від Надавача або за результатами його перевірки, відомостей про порушення конфіденційності та/або цілісності інформації, що впливають на надання електронних довірчих послуг або стосуються персональних даних користувачів;
- видає приписи щодо усунення порушень вимог законодавства у сфері електронних довірчих послуг;
- накладає адміністративні штрафи за порушення вимог законодавства у сфері електронних довірчих послуг;
- аналізує документи про відповідність за результатами проведення процедур оцінки відповідності Надавача у рамках невиїзних заходів державного нагляду (контролю).

1.4. Використання сертифіката

Використання сертифіката здійснюється відповідно до положень пункту 5.5 ДСТУ ETSI EN 319 411-1

Крім того, застосовуються такі особливі вимоги:

1.4.1. Дозволене використання сертифіката

1.4.1.1. Види кваліфікованих сертифікатів

Надавач формує кваліфіковані сертифікати наступних 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.

1.4.1.2.Строк дії кваліфікованих сертифікатів

Кваліфіковані сертифікати Надавача формуються ЦЗО зі строком дії не більше п’яти років.

Строк дії кваліфікованих сертифікатів Надавача становить п’ять років для наступних типів сертифікатів:

- особистого ключа Надавача 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;
- CMP з параметрами, що відповідають таким вимогам: алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;
- TSP з параметрами, що відповідають таким вимогам: алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;

- OCSP з параметрами, що відповідають таким вимогам: алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002.

Кваліфіковані сертифікати користувачів формуються Надавачем зі строком дії 1 або 2 роки.

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

1.4.2. Заборонене використання сертифіката

Кваліфікований сертифікат може використовуватися лише відповідно до зазначеного у ньому призначення відкритого ключа.

1.4.3. Використання тестових сертифікатів

Формування тестових сертифікатів здійснюється Надавачем через інтеграцію з програмним інтерфейсом, створеним на офіційному веб-сайті ЦЗО в рамках інструменту моніторингу сфери електронних довірчих послуг 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.

1.5. Управління Політикою сертифіката

1.5.1. Відповідальність за Політику сертифіката

Ця Політика сертифіката підтримується Товариством з обмеженою відповідальністю «Арт-мастер» (далі – ТОВ «Арт-мастер»).

ТОВ «Арт-мастер» є зареєстрованою відповідно до законодавства юридичною особою.

Головний офіс Надавача представлений функціональним підрозділом ТОВ «Арт-мастер», що здійснює організацію надання кваліфікованих електронних довірчих послуг КНЕДП «MASTERKEY» та відокремленими пунктами реєстрації КНЕДП «MASTERKEY» та забезпечує виконання вимог законодавства до кваліфікованих надавачів електронних довірчих послуг. Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені ТОВ «Арт-мастер».

Реквізити ТОВ «Арт-мастер»:
- Код ЄДРПОУ: 30404750
- Юридична адреса: 03035, місто Київ, вул. Монастирського Дениса, 3
- Телефон: +38 (044) 206-13-78
- Електронна пошта: help@am-soft.ua

Реквізити КНЕДП «MASTERKEY»:
- Веб-сайт: https://ca.masterkey.ua
- Електронна пошта: info@masterkey.ua

Ця Політика сертифіката, а також зміни до неї затверджується директором ТОВ «Арт-мастер».

Ця Політика сертифіката, а також зміни до неї 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 Політики сертифіката

Внесення змін до цієї Політики сертифіката здійснюється у разі:
- змін вимог, процесів та процедур описаних в цій Політиці сертифіката;
- змін у вимогах до надавачів щодо надання послуг;
- змін в законодавстві.

1.6. Визначення термінів та перелік скорочень

1.6.1. Визначення термінів

У цій Політиці сертифіката використано терміни, встановлені в Законі України «Про електронну ідентифікацію та електронні довірчі послуги» та документах, зазначених у п. 3 Регламенту Надавача.

1.6.2. Перелік скорочень

ВПР	Відокремлений пункт реєстрації
ДРФО	Державний реєстр фізичних осіб - платників податків
ЄДДР	Єдиний державний демографічний реєстр
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань
ІКС	Інформаційно-комунікаційна система
КЗІ	Криптографічній захист інформації
КО	Контролюючий орган
КСЗІ	Комплексна система захисту інформації
ООВ	Орган з оцінки відповідності
ЦЗО	Центральний засвідчувальний орган
CMP	Certificate Management Protocol (Протокол управління сертифікатами)
OCSP	Online Certificate Status Protocol (протокол визначення статусу сертифіката ключа)
OLS	Online Service (Онлайн сервіс)
TSP	Time Stamp Protocol (протокол позначки часу)

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

Крім того, застосовуються такі особливі вимоги:

2.1. Репозиторій/Веб-сайт

Надавач забезпечує:

- створення та функціонування веб-сайту Надавача;
- впровадження, підтримання в актуальному стані та публікацію на веб-сайті Надавача 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.

Надавач також повинен забезпечувати інформування користувачів про умови отримання кваліфікованих електронних довірчих послуг шляхом розміщення відповідної інформації на веб-сайті Надавача.

Перелік інформації, що розміщується Надавачем на своєму офіційному веб-сайті:

- відомості про Надавача, в тому числі про ВПР Надавача, в обсязі, достатньому для їх однозначного встановлення користувачем (реквізити, адреси, контактні телефони, режими роботи тощо);
- інформація про внесення Надавача до Довірчого списку;
- перелік кваліфікованих електронних довірчих послуг, які надає Надавач;
- кваліфіковані сертифікати відкритих ключів Надавача;
- кваліфіковані сертифікати відкритих ключів користувачів (за згодою користувачів);
- списки відкликаних сертифікатів відкритих ключів;
- відомості про обмеження під час використання кваліфікованих сертифікатів відкритих ключів користувачами;
- перелік, форми документів, на підставі яких надаються електронні довірчі послуги, та роз’яснення щодо їх оформлення;
- дані про засоби кваліфікованого електронного підпису та печатки, що використовуються під час надання електронних довірчих послуг;
- дані про порядок перевірки чинності кваліфікованого сертифіката відкритого ключа, у тому числі умови перевірки статусу кваліфікованого сертифіката відкритого ключа;
- перелік нормативно-правових актів у сфері електронних довірчих послуг, Регламент Надавача з Політикою сертифіката та Положенням сертифікаційних практик.

Ця Політика сертифіката доступна 24 години на добу 7 днів на тиждень на веб-сайті Надавача.

2.2. Публікація інформації

2.2.1. Публікація 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 електронних довірчих послуг.

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

2.2.2. Публікація сертифікатів Надавача

Кваліфіковані сертифікати відкритих ключів Надавача публікуються одразу після їх отримання від ЦЗО.

Кваліфіковані сертифікати відкритих ключів серверів Надавача публікуються одразу після їх формування Надавачем.

2.2.3. Доступ до сертифікатів Користувачів

Кваліфікований сертифікат Користувача після його формування Надавачем повинен бути доступний Користувачу, для якого такий сертифікат був сформований.

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

2.2.4. Строк закінчення дії сертифіката

Строк дії кваліфікованих сертифікатів користувачів електронних довірчих послуг Надавача становить не більше двох років.

Строк дії кваліфікованих сертифікатів Надавача становить п’ять років для наступних типів сертифікатів:

- особистого ключа Надавача з параметрами, що відповідають таким вимогам: алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;
- CMP з параметрами, що відповідають таким вимогам: алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;
- TSP з параметрами, що відповідають таким вимогам: алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;
- OCSP з параметрами, що відповідають таким вимогам: алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002.

2.3. Час та періодичність публікації

Кваліфіковані сертифікати відкритих ключів Надавача публікуються одразу після їх отримання від ЦЗО.

Кваліфіковані сертифікати відкритих ключів серверів Надавача публікуються одразу після їх формування Надавачем.

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

2.4. Контроль доступу до репозиторію/веб-сайту

Репозиторій/веб-сайт захищений від несанкціонованого доступу та змін. Надавач забезпечує цілодобове функціонування власного репозиторію/веб-сайту.

За захист інформації на репозиторію/веб-сайті Надавача відповідає позаштатна служба захисту інформації ТОВ «Арт-мастер», визначена наказом про створення служби захисту інформації.

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

3.1. Позначення

Кваліфіковані сертифікати обов'язково повинні містити відомості, визначені частиною другою статті 23 Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

Кваліфіковані сертифікати можуть містити відомості про обмеження використання кваліфікованого електронного підпису чи печатки.

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 кваліфікованих електронних підписів чи печаток.

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

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 цієї 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 цієї Політики сертифіката.

3.1.3. Використання псевдонімів

Процедура використання псевдонімів здійснюється відповідно до Порядку використання псевдонімів фізичними особами, які є користувачами послуг електронної ідентифікації або електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 28.06.2024 №764 «Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг»

3.1.4. Правила інтерпретації різних форм позначень сертифіката

Міжнародні літери повинні кодуватися згідно з UTF-8.

3.1.5. Унікальність позначень сертифіката

Надавач повинен переконатися, що сертифікати з однаковими даними, зазначеними в полях «Повне ім’я/найменування користувача» («Common Name») та «Серійний номер» («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

Крім того, застосовуються такі особливі вимоги:

3.2.1. Метод підтвердження володіння особистим ключем

Підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа забезпечується одним з таких методів:

- візуальним та технічним контролем запису та передачі Надавачу запиту на формування кваліфікованого сертифіката відкритого ключа, особисто користувачем під час генерації пари ключів, одразу після ідентифікації користувача, за умови його особистої присутності;
- технічним контролем запису та передачі Надавачу запиту на формування кваліфікованого сертифіката відкритого ключа

користувачем, під час генерації пари ключів, одразу після ідентифікації користувача за ідентифікаційними даними, що містяться у раніше сформованому Надавачем кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката.

При застосуванні будь якого з двох наведених методів, за допомогою засобів електронного підпису Надавача, здійснюється перевірка 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

На виконання положень Статті 22 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» під час формування та видачі кваліфікованого сертифіката відкритого ключа Надавач обов'язково здійснює встановлення (ідентифікацію) особи.

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

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

1) за особистої присутності фізичної особи, фізичної особи - підприємця чи уповноваженого представника юридичної особи - за результатами перевірки відомостей 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;
2) за ідентифікаційними даними особи, що містяться у кваліфікованому сертифікаті електронного підпису чи печатки, раніше сформованого (сформованої) та виданого (виданої) згідно з пунктом 1 цієї частини, за умови чинності такого сертифіката.

Ідентифікація іноземців здійснюється відповідно до законодавства України.

Надавач також може здійснювати перевірку чинності документів наданих фізичною особою за даними щодо недійсних документів на інформаційному ресурсі Державної міграційної служби України.

Для здійснення перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи – підприємця, Надавач зобов'язаний використовувати інформацію, що міститься в ЄДР та пересвідчитися, що обсяг цивільної правоздатності та дієздатності є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа.

Під час встановлення особи Надавач може використовувати засоби фото або відео фіксації для підтвердження факту пред'явлення користувачем документів, що посвідчують особу. Збереження фото або відео фіксації в ІКС надавача здійснюється з урахуванням положень законодавства України в сфері захисту інформації та захисту персональних даних.

3.2.3. Неперевірена інформація про користувача

Неперевірена інформація про користувача не допускається.

Відповідні Положення сертифікаційних практик Надавача містять додаткову інформацію.

3.2.4. Підтвердження повноважень

Уповноважений представник юридичної особи або фізична особа - підприємець підписує документи, необхідні для формування та видачі кваліфікованого сертифіката працівнику юридичної особи або фізичної особи - підприємця.

Надавач, перед формуванням кваліфікованого сертифіката відкритого ключа здійснює ідентифікацію особи уповноваженого представника юридичної особи відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги», а також перевіряє обсяг його повноважень за документом та/або за даними ЄДР, що визначають повноваження представника.

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, договорі, довіреності тощо.

Надання електронних довірчих послуг Надавачем, передбачає проведення ідентифікації користувачів під час опрацювання заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів.

Для ідентифікації особи користувача, що звернувся до Надавача для отримання електронних довірчих послуг, Надавач вимагає разом із заявою надати, а користувач надає документи що містять інформацію, яка вноситься до кваліфікованого сертифіката відкритого ключа.

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

3.3.1. Ідентифікація та автентифікація користувача за заявою про формування сертифіката за умови чинності попереднього сертифіката

Користувачі, які установленим порядком пройшли реєстрацію та володіють чинними, незаблокованими та не анульованими сертифікатами, можуть в автоматизованому режимі здійснити переоформлення таких сертифікатів, та/або здійснювати повторне формування сертифікатів, пов'язане з закінченням терміну дії чинних сертифікатів, шляхом розміщення на електронному ресурсі сервісу «OLS» Надавача електронних документів та електронних копій документів, виготовлених скануванням оригіналів документів на паперових носіях.

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 на момент подання заяви сертифіката ключа, що містить ідентифікаційні дані особи.

3.3.2. Ідентифікація та автентифікація користувача на отримання повторного формування кваліфікованого сертифіката відкритого ключа у разі скасування сертифіката

У разі, якщо кваліфікований сертифікат користувача скасовано, для формування нового кваліфікованого сертифіката у Надавача користувач повинен пройти ідентифікацію та автентифікацію згідно з умовами для первинної ідентифікації та автентифікації користувача визначених підпунктом 1 пункту 3.2.2 цієї Політики сертифіката.

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

Перелік та опис механізмів ідентифікації та автентифікації користувачів з питань скасування, блокування або поновлення кваліфікованого сертифіката відкритого ключа наведено у Таблиці 1:

Таблиця 1

Перелік
механізмів ідентифікації та автентифікації користувачів

Найменування дії зі зміни статусу сертифікату	Форма звернення	Механізми ідентифікації та автентифікації
Скасування кваліфікованого сертифіката відкритого ключа	Письмова	Аналогічний механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа
	Електронна	Аналогічний механізмам підтвердження ідентифікаційних даних Користувачів, які мають чинний кваліфікований сертифікат відкритого

		ключа, сформований Надавачем
Блокування кваліфікованого сертифіката відкритого ключа	Усна	За ключовою фразою голосової автентифікації, первинний обмін якою між Надавачем та користувачем здійснюється під час подання заяви про формування кваліфікованого сертифіката відкритого ключа
	Письмова	Аналогічний механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа
	Електронна	Аналогічний механізмам підтвердження ідентифікаційних даних Користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований Надавачем
Поновлення кваліфікованого сертифіката відкритого ключа	Письмова	Аналогічний механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа

Перевірка ідентифікаційних даних користувача, який звертається із заявою про блокування або скасування кваліфікованого сертифіката в електронній формі, а також законності такого звернення, здійснюється шляхом автентифікації та ідентифікації користувача на електронному сервісі «OLS» Надавача за допомогою чинного кваліфікованого сертифіката користувача, що містить ідентифікаційні дані особи на момент подання заяви.

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

4.1. Запит на сертифікат

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

Запит на формування кваліфікованого сертифіката приймається в обробку після приймання та реєстрації заяви на формування кваліфікованого сертифіката, ідентифікації та автентифікації особи користувача та підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката.

4.2. Обробка запиту на сертифікат

Для формування кваліфікованих сертифікатів при отриманні користувачем електронних довірчих послуг використовуються запити на формування кваліфікованих сертифікатів підпису, які створюються в процесі генерації особистого та відкритого ключів.

Якщо генерація особистих та відкритих ключів була проведена за межами приміщення Надавача, запити на сертифікацію надаються адміністратору сертифікації особисто користувачем через онлайн сервіс «OLS» або виїзним адміністратором, який здійснював реєстрацію.

Підтвердження володіння користувачем відповідним особистим ключем та його відповідність відкритому ключу здійснюється адміністратором реєстрації без розкриття особистого ключа користувача, шляхом перевірки кваліфікованого підпису та печатки на запиті за допомогою відкритого ключа, що міститься у запиті.

В процесі генерації ключів створюється особистий та відкритий ключ та запит на формування сертифікату. Запит на формування сертифіката ключа, що передається на сертифікацію до Надавача, є самопідписаним запитом формату PKCS#10. Особистий ключ Надавачу не передається та зберігається у користувача.

Під час обробки запиту на формування сертифіката ключа здійснюється перевірка відповідності особистого ключа користувача відкритому ключу, який міститься у запиті. Перевірка здійснюється автоматично з використанням програмного забезпечення ІКС Надавача. Формування сертифіката ключа можливе лише за умови позитивного результату перевірки.

Строк обробки запиту на формування кваліфікованого сертифіката, поданого разом із заявою на реєстрацію, залежить від обраного користувачем пакета послуг і становить не більше 48 годин після внесення оплати за послугу.

4.3. Формування сертифіката

Надання сформованого кваліфікованого сертифіката відкритого ключа користувачу здійснюється в один із способів:

- надсилання файлу із сформованим кваліфікованим сертифікатом відкритого ключа на адресу електронної пошти, вказану у заяві на формування кваліфікованого сертифіката відкритого ключа;
- запису файлу із сформованим кваліфікованим сертифікатом відкритого ключа на носій інформації, наданий користувачем;
- публікації сформованого кваліфікованого сертифіката відкритого ключа на офіційному інформаційному ресурсі Надавача.

4.4. Прийняття сертифіката

Публікації сформованого кваліфікованого сертифіката відкритого ключа на офіційному інформаційному ресурсі Надавача відбувається одразу після обробки запиту на сертифікат.

Користувач повинен перевірити свої ідентифікаційні дані, внесені до кваліфікованого сертифіката Надавачем. Надавач повинен надавати відповідні консультації щодо проведення такої перевірки.

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

У разі невідповідності ідентифікаційних даних, внесених Надавачем до кваліфікованого сертифіката та виявлених користувачем після отримання сформованого кваліфікованого сертифіката, власник такого сертифіката особисто звертається до Надавача для скасування цього сертифіката та формування нового кваліфікованого сертифіката у встановленому порядку.

У разі невідповідності ідентифікаційних даних, внесених Надавачем до кваліфікованого сертифіката відкритого ключа та виявлених Надавачем до моменту надання сформованого сертифіката користувачу, Надавачем здійснюється переформування сертифікату із використанням попередньо засвідченого відкритого ключа та з дотриманням вимог щодо недопущення перевищення встановленого строку чинності особистого ключа та відповідного йому відкритого ключа.

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

4.5.1. Використання особистого ключа та сертифіката користувачем

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

- забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;
- використовувати особистий ключ виключно з метою, визначеною у кваліфікованому сертифікаті;
- не використовувати особистий ключ у разі його компрометації, скасування чи блокування;

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

- цієї Політики сертифіката;
- Положення сертифікаційних практик КНЕДП «MASTERKEY»;
- Загальних положень Регламенту Надавача;
- Договору про надання електронних довірчих послуг, укладеного з ТОВ «Арт-мастер».

4.5.2. Використання відкритого ключа та сертифіката суб’єктами, які довіряють Надавачу

Кваліфіковані сертифікати користувачів, сформовані Надавачем, можуть використовуватися будь-якими суб’єктами, які довіряють Надавачу, з метою їх автентифікації, за умовою перевірки наступної інформації:

- статус кваліфікованого сертифіката користувача. Перевіряється за допомогою OCSP-серверу Надавача;

- сферу використання кваліфікованого сертифіката користувача згідно поля «KeyUsage» в сертифікаті;
- відповідність особистого ключа кваліфікованого електронного підпису чи печатки відкритому ключу зазначеному в кваліфікованому сертифікаті користувача.

Кваліфікований електронний підпис чи печатка вважаються дійсними, коли здійснені результати перевірки в наведених вище пунктах виконані успішно та є дійсними одночасно.

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

4.6. Поновлення сертифіката

Поновлення сертифіката можливе лише для заблокованих сертифікатів виданих Надавачем, термін дії яких не закінчився та термін блокування яких не перевищує 30 календарних днів з моменту блокування. Скасовані сертифікати поновленню не підлягають.

Надавач зобов'язаний поновити заблокований сертифікат в наступних випадках:

- подання користувачем електронних довірчих послуг заяви про поновлення його заблокованого кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи користувача (якщо блокування здійснено на підставі заяви про блокування кваліфікованого сертифіката відкритого ключа);
- встановлення недостовірності відомостей про компрометацію відповідного особистого ключа;
- набрання законної сили рішенням суду про поновлення сертифіката;
- в інших випадках, передбачених чинним законодавством України.

Прийняття заяви на поновлення сертифіката ключа здійснюються згідно графіка роботи Надавача та його відокремлених пунктів реєстрації.

Опрацювання заяви на поновлення чинності сертифіката та інформування користувача про поновлення здійснюється протягом двох годин з моменту отримання заяви Надавачем.

4.7. Повторне формування сертифіката

Повторне формування сертифіката ключа здійснюється за зверненням користувача у разі:

- наближення строку завершення чинності сертифіката, з генерацією нових відкритого та особистого ключів;
- зміни відомостей, зазначених у сертифікаті ключа, впродовж дії договору про обслуговування сертифіката, необхідність генерації нових

відкритого та особистого ключів встановлює користувач. Попередній сертифікат ключа в такому разі автоматично скасовується;
- прийняття користувачем такого рішення. Необхідність генерації нових відкритого та особистого ключів встановлює користувач.

Обслуговування користувачів при повторному формуванні сертифікатів може здійснюватися за процедурами, ідентичними процедурам при первинному формуванні сертифіката, або за наявності чинного кваліфікованого сертифікату, що містить ідентифікаційні дані користувача, в автоматизованому режимі (з використанням сервісу «OLS» Надавача).

4.8. Зміна сертифіката

Внесення змін до кваліфікованого сертифіката не допускається.

4.9. Скасування та блокування сертифіката

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

Надавач здійснює цілодобовий прийом електронних заяв користувачів про скасування та блокування їхніх кваліфікованих сертифікатів, сформованих Надавачем, за допомогою сервісу «OLS»

Прийом та перевірку заяв у паперовій формі користувачів про скасування та блокування їхніх кваліфікованих сертифікатів, сформованих Надавачем, здійснюється протягом робочого дня згідно графіка роботи Надавача та його відокремлених пунктів реєстрації.

Скасування та блокування кваліфікованих сертифікатів, сформованих Надавачем, відбувається відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Блокування сертифіката ключа може здійснюватися на підставі заяви, поданої користувачем в усній формі за ключовою фразою голосової автентифікації, яка була зазначена під час подання заяви про формування кваліфікованого сертифіката або за паперовою заявою. 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 кваліфікованого сертифіката (відповідно до пункту 4.6. цієї Політики сертифіката). Блокований кваліфікований сертифікат буде автоматично скасований Надавачем, 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.

Надавач формує списки відкликаних сертифікатів (CRL) у вигляді повного та часткового списку, які відповідають таким вимогам:

- повний список відкликаних сертифікатів випускається не рідше 1 (одного) разу на тиждень та містить інформацію про всі відкликані сертифікати ключів, які були сформовані Надавачем;
- частковий список відкликаних сертифікатів випускається кожні 2 (дві) години та містить інформацію про усі відкликані сертифікати ключів, статус яких був змінений в інтервалі між часом випуску останнього повного списку та часом формування поточного часткового списку;
- в кожному списку обов’язково зазначається точна дата та час публікації наступного списку;
- новий список може бути опублікований до визначеного часу видання наступного списку, вказаного у поточному списку відкликаних сертифікатів.

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

Посилання на списки відкликаних сертифікатів вносяться до кваліфікованих сертифікатів користувачів.

4.10. Служби статусу сертифіката

Надавач надає усім користувачам послугу інтерактивного визначення статусу сертифіката сформованого КНЕДП «MASTERKEY». Послуга надається шляхом відправлення запиту на OCSP-сервер Надавача.

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

Контроль фізичної безпеки здійснюється відповідно до положень пункту 6.4.2 ДСТУ ETSI EN 319 411-1

Крім того, застосовуються такі особливі вимоги:

5.1.1. Вимоги до приміщень Надавача

В приміщеннях, в яких розташовані компоненти ІКС, повинен діяти пропускний та внутрішньо об'єктовий режими, забезпечуватися контроль виконання пропускного та внутрішньо об'єктового режимів, протипожежної безпеки в межах контрольованої території, а також цілодобовий контроль доступу в приміщення, в яких розташовані компоненти майданчика ІКС.

Розділ приміщень Надавача на функціональні зони за рівнями безпеки приміщень визначається організаційно-розпорядчим документом Надавача.

Для кожного рівня безпеки приміщень визначено мінімально необхідний набір механізмів безпеки, зокрема: контролю доступу, виявлення вторгнень, пожежної сигналізації та пожежогасіння, альтернативних та резервних джерел електроживлення тощо.

5.1.2. Фізичний доступ

В будівлі, де знаходяться технічні засоби ІКС, функціонує система контролю доступу до контрольованої території майданчику.

Контрольована територія обмежена системою контролю доступу на вході у відповідне приміщення та зовнішніми стінами.

Доступ до компонентів ІКС має лише обслуговуючий персонал відповідно до своїх службових обов'язків. Доступ інших осіб до компонентів ІКС можливий лише в супроводі осіб, яким надано такий доступ.

Доступ в приміщення, які призначені для обслуговування користувачів – вільний, під контролем працівників Надавача.

5.2. Процедурний контроль

Процедурний контроль здійснюється відповідно до вимог, визначених в пункті 6.4.3 ДСТУ ETSI EN 319 411-1.

5.3. Контроль персоналу

Контроль персоналу здійснюється відповідно до вимог, визначених в пункті 6.4.4 ДСТУ ETSI EN 319 411-1, а також відповідно до посадових інструкцій Надавача, що є складовою документації КСЗІ ІКС Надавача.

5.3.1. Довірені ролі персоналу

Персоналом Надавача є:

- керівник Надавача;
- адміністратор реєстрації;
- адміністратор сертифікації;
- адміністратор безпеки;
- аудитор системи;
- системний адміністратор.

5.3.1.1. Керівник

Керівник Надавача в межах виконання своїх обов'язків відповідає за організацію та контроль процесів, направлених на забезпечення функціонування, розвитку Надавача та захист інформації в ІКС Надавача, а саме:

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

5.3.1.2. Адміністратор реєстрації

Адміністратор реєстрації відповідає за перевірку документів, наданих користувачами, їх заяв про формування, блокування, поновлення та скасування кваліфікованих сертифікатів.

Основними обов’язками адміністратора реєстрації є:

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

Додатковими обов’язками адміністратора реєстрації є:

- надання допомоги під час генерації пари ключів користувача;
- обробка запитів на формування та зміну статусу сертифікатів ключів користувачів;

- надання консультацій щодо умов та порядку отримання кваліфікованих електронних довірчих послуг;
- ведення архіву Надавача.

До працівників відокремлених пунктів реєстрації Надавача, на яких покладено обов'язки з реєстрації користувачів, повинні застосовуватись такі ж вимоги, як і до адміністраторів реєстрації.

5.3.1.3. Адміністратор сертифікації

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

Основними обов'язками адміністратора сертифікації є:

- участь у генерації пар ключів Надавача та створенні резервних копій особистих ключів Надавача;
- зберігання особистих ключів Надавача та їх резервних копій;
- забезпечення використання особистих ключів Надавача під час формування та обслуговування кваліфікованих сертифікатів Надавача та користувачів;
- перевірка заяв про формування кваліфікованих сертифікатів Надавача на відповідність вимогам цієї Політики сертифікації та відповідних Положень сертифікаційних практик;
- участь у знищенні особистих ключів Надавача;
- забезпечення ведення, архівування та відновлення баз даних кваліфікованих сертифікатів користувачів;
- забезпечення публікації кваліфікованих сертифікатів користувачів та списків відкликаних сертифікатів на веб-сайті Надавача;
- створення резервних копій кваліфікованих сертифікатів користувачів;
- зберігання кваліфікованих сертифікатів відкритих ключів користувачів, їх резервних копій, списків відкликаних сертифікатів та інших важливих ресурсів ІКС Надавача.

5.3.1.4. Адміністратор безпеки

Адміністратор безпеки відповідає за належне функціонування КСЗІ в ІКС Надавача.

Основними обов'язками адміністратора безпеки є:

- участь у генерації пар ключів Надавача та створенні резервних копій особистих ключів Надавача;
- контроль за формуванням, обслуговуванням, створенням та перевіркою резервних копій кваліфікованих сертифікатів Надавача, користувачів та списків відкликаних сертифікатів;

- контроль за зберіганням особистих ключів Надавача та їх резервних копій, особистих ключів адміністраторів;
- участь у знищенні особистих ключів Надавача, контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;
- організація розмежування доступу до ресурсів ІКС Надавача;
- забезпечення спостереження за функціонуванням ІКС Надавача (реєстрація подій в ІКС Надавача, моніторинг подій тощо);
- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування ІКС Надавача після збоїв, відмов;
- забезпечення режиму доступу до приміщень Надавача, в яких розміщена ІКС Надавача;
- контроль за дотриманням персоналом Надавача положень внутрішньої організаційно-розпорядчої документації Надавача та документації КСЗІ;
- контроль за веденням баз даних Надавача.

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

5.3.1.5.Системний адміністратор

Системний адміністратор відповідає за функціонування технічних засобів ІКС Надавача.

Основними обов'язками системного адміністратора є:

- організація експлуатації та технічного обслуговування ІКС Надавача і адміністрування її технічних засобів;
- забезпечення функціонування веб-сайту Надавача;
- участь у впровадженні та забезпеченні функціонування КСЗІ в ІКС Надавача;
- ведення журналів аудиту подій, що реєструють технічні засоби ІКС Надавача;
- встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення ІКС Надавача;
- встановлення та налагодження штатної підсистеми резервного копіювання бази даних ІКС Надавача;
- забезпечення актуалізації баз даних, створюваних та оброблюваних в ІКС Надавача, у зв'язку із збоями.

5.3.1.6.Аудитор системи

Аудитор системи відповідає за належне функціонування ІКС Надавача.

Основними обов'язками аудитора системи є:

- проведення перевірок журналів аудиту подій, що реєструють технічні засоби та обладнання програмно-технічного комплексу ІКС Надавача;
- контроль за веденням архіву Надавача.

5.3.2. Вимоги щодо кваліфікації, досвіду та допуску персоналу

Персонал Надавача повинен мати необхідні для надання кваліфікованих електронних довірчих послуг знання, досвід і кваліфікацію та дотримуватись положень внутрішньої організаційно-розпорядчої документації та вимог КСЗІ.

5.3.3. Вимоги та процедури навчання персоналу

Керівник Надавача зобов'язаний забезпечити створення умов для безперервної особистої освіти та постійне підвищення кваліфікації персоналу Надавача у сферах інформаційних технологій, захисту інформації або кібербезпеки та захисту персональних даних.

Персонал Надавача регулярно бере участь в семінарах, конференціях та зустрічах щодо надання кваліфікованих електронних довірчих послуг, інформаційних технологій, захисту інформації, кібербезпеки та захисту персональних даних.

5.3.4. Санкції за несанкціоновані дії персоналу

Керівником Надавача встановлена чітка система дисциплінарних стягнень за недотримання персоналом Надавач своїх посадових обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг і вимог внутрішньої організаційно-розпорядчої документації Надавача.

Недотримання персоналом Надавача своїх посадових обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг, вимог внутрішньої організаційно-розпорядчої документації Надавача передбачає дисциплінарні стягнення, адміністративну та кримінальну відповідальність, передбачені такими документами:

- посадовою інструкцією;
- трудовим договором;
- договором на здійснення представництва Надавача (для відокремлених пунктів реєстрації Надавача, що працюють за агентським договором);
- Кодексом України про адміністративні правопорушення;
- Кримінальним кодексом України.

5.3.5. Контроль відокремлених пунктів реєстрації

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

До складу працівників відокремлених пунктів реєстрації Надавача, входять працівники Надавача або працівники юридичних осіб та фізичні особи - підприємці, які на підставі договору з Надавачем здійснюють реєстрацію користувачів.

На працівників відокремлених пунктів реєстрації Надавача покладено такі функціональні обов’язки:

- адміністратора реєстрації;
- відповідального за захист інформації на відокремленому пункті реєстрації, в тому числі за захист персональних даних підписувачів.

5.3.6. Документація, яка надається персоналу

Організаційно-правовий статус керівника профільного підрозділу і персоналу Надавача, їх завдання та функції, права та обов’язки, відповідальність, а також професійні знання, досвід і кваліфікація визначаються у посадових інструкціях.

Посадові інструкції повинні містити вимоги інформаційної безпеки та методи її забезпечення.

Керівник і персонал Надавача повинні бути ознайомлені з положеннями їх посадових інструкцій.

Персонал Надавача повинен бути повідомлений про зміни в організації процесів Надавача, що стосуються їх посадових обов’язків.

5.4. Ведення журналу аудиту подій

Ведення журналу аудиту подій здійснюється відповідно до вимог, визначених в пункті 6.4.5 ДСТУ ETSI EN 319 411-1

5.4.1. Типи записаних подій

Надавачем, за допомогою спеціального програмного забезпечення, здійснюється автоматична реєстрація та внесення до електронних журналів ІКС таких подій:

- спроби створення, знищення, встановлення паролів, зміни прав доступу в ІКС;
- заміни програмного забезпечення, технічних засобів ІКС;
- технічне обслуговування ІКС;
- генерація, використання, знищення особистих ключів Надавача;
- формування, блокування, скасування та поновлення сертифікатів відкритих ключів, формування списків відкликаних сертифікатів відкритих ключів;
- спроби несанкціонованого доступу до ІКС;
- надання доступу персоналу до ІКС;
- збоїв в роботі ІКС;
- інші події, необхідні для формування доказової бази при розгляді судових справ.

5.4.2. Частота обробки журналу аудиту подій

Журнали аудиту подій, що ведуться в ІКС, переглядаються аудитором системи періодично, але не рідше одного разу на тиждень з метою виявлення подій (серед зареєстрованих у журналі аудиту), які свідчать про ситуацію, яка призвела або може призвести до порушення безпеки експлуатації ІКС.

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

5.4.3. Строки зберігання журналу аудиту подій

Журнали аудиту подій, зберігаються протягом 10 років у місці їх створення, після чого забезпечується їх передача на архівне зберігання.

5.4.4. Захист журналу аудиту подій

Усі записи в журналах аудиту подій в електронній формі повинні містити дату та час події, а також ідентифікувати суб'єкта, що її ініціював або брав у ній участь.

Час, що зазначається у журналі аудиту подій, повинен бути синхронізований із Всесвітнім координованим часом (UTC) з точністю до секунди.

Журнали аудиту подій повинні бути захищені від неавторизованого перегляду, модифікації і знищення.

5.4.5. Процедури резервного копіювання журналу аудиту подій

Резервне копіювання журналів аудиту здійснюється раз на добу, резервне копіювання журналів аудиту на знімні носії здійснюється раз на тиждень.

Резервні копії журналів аудиту подій на знімних носіях зберігаються в окремому приміщенні із забезпеченням їх захисту від несанкціонованого доступу.

Резервування здійснюється системним адміністратором відповідними засобами, що входять до складу ІКС, під контролем та за участю аудитора системи. Факти проведення резервування протоколюються (за період) та засвідчуються підписами відповідальних осіб. Управління доступом до резервних копій журналів аудиту та контроль за їх зберіганням та застосуванням здійснює адміністратор безпеки.

5.4.6. Синхронізація часу

Синхронізація часу у технічних засобах ІКС Надавача відбувається відповідно до Порядку синхронізації часу, погодженого з ЦЗО.

Основним джерелом часу для ІКС Надавача є NTP-сервери ЦЗО.

5.5. Архів документів

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.4.6 ДСТУ ETSI EN 319 411-1

5.5.1. Види документів та даних, що підлягають архівному зберіганню

Види документів та даних, що підлягають архівуванню, а також механізм та форма зберігання архівів наведено у Таблиці 2:

Таблиця 2

Види документів та даних, що підлягають архівуванню

Види документів та даних	Форма зберігання	Механізм зберігання
Кваліфіковані сертифікати відкритих ключів Надавача, серверів Надавача, посадових осіб Надавача, користувачів та створювачів електронних печаток	Електронна	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
Журнали аудиту подій ІКС Надавача	Електронна	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
	Паперова	Сховище (сейф)
Укладені договори про надання електронних довірчих послуг	Електронна	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
Заяви на формування кваліфікованих сертифікатів відкритих ключів та зміну статусу сертифікатів, копії документів, що використовуються під час реєстрації користувачів	Електронна	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації
Список відкликаних кваліфікованих сертифікатів відкритих ключів, повний та частковий	Електронна	Автоматичне резервне копіювання засобами ІКС Надавача та ручне архівне копіювання на окремі носії інформації

5.5.2. Строки зберігання архіву

Усі кваліфіковані сертифікати, списки відкликаних сертифікатів та журнали аудиту подій підлягають постійному зберіганню.

Документи у паперовому та електронному вигляді, мають зберігатися у порядку, встановленому законодавством про архіви та архівні справи.

5.5.3. Захист архіву

Для зберігання носіїв з архівними копіями електронних документів виділяється окреме сховище (сейф чи відсік сейфу) з двома екземплярами ключів. Один екземпляр ключа від сховища знаходиться у адміністратора

безпеки, а другий - в опечатаному конверті зберігається у сховищі (сейфі) керівника Надавача.

5.5.4. Процедури резервного копіювання архіву

Автоматичне резервне копіювання даних забезпечується засобами, що входять до складу ІКС Надавача. Автоматичне створення резервної копії має виконуватися не рідше одного разу на добу, під час найменшого завантаження ІКС.

Резервне копіювання даних на знімні носії інформації виконуватися у ручному режимі. Після створення нової резервної копії, попередня резервна копія стає архівною.

Відновлення даних з резервної копії здійснюються засобами ІКС, шляхом зчитування з останньої (актуальної) резервної копії та запису їх у базу даних сервера.

Знімні носії із архівними копіями зберігаються у конвертах чи упаковках, що засвідчуються підписом адміністратора аудиту. При цьому на упаковці вказується обліковий номер копії. Факти створення та використання копій фіксуються у окремому журналі.

Журнали аудиту подій мають зберігатися в приміщенні Надавача. Контроль за здійсненням автоматичного резервного копіювання та виконання резервного копіювання в ручному режимі покладається на системного адміністратора. Аудитор системи періодично контролює процес створення та зберігання резервних копій.

5.5.5. Вимога щодо накладання електронних позначок часу на записи

Надавач за необхідності може накладати електронні позначки часу на записи, пов’язані з його діяльністю.

5.5.6. Система збирання архівів (внутрішня чи зовнішня)

Системи збору архівів знаходяться в службових та спеціальних приміщеннях Надавача.

Вимоги до службових та спеціальних приміщень описані в пункті 5.1.1 цієї Політики сертифіката.

5.5.7. Процедури отримання та перевірки архівної інформації

Доступ до архівних даних суворо обмежений. Доступ до цієї системи мають лише уповноважені працівники згідно із службовими повноваженнями. Надавач оприлюднює інформацію з архіву лише за рішенням суду.

5.6. Зміна ключа

Зміна ключа Надавача та ключів його сервісів CMP, OCSP, TSP може бути планова або позапланова.

Планова зміна ключів Надавача виконується не пізніше ніж за два роки до завершення строку дії кваліфікованого сертифіката Надавача.

Генерації та резервному копіюванню підлягають особистий ключ Надавача, ключ сервера запитів управління сертифікатами (CMP-сервера), ключ сервера визначення статусу сертифікатів (OCSP-сервера) та ключ сервера позначок часу (TSP-сервера).

Під час процедури планової зміни ключів Надавача застосовуються наступний порядок дій та вимог:

- генерація особистих ключів Надавача та особистих ключів серверів Надавача виконується засобами кваліфікованого електронного підпису зі складу ІКС, у спеціальному приміщенні Надавача адміністратором сертифікації під контролем адміністратора безпеки;
- згенерований особистий ключ Надавача під час експлуатації ПТК ІКС знаходиться у постійному запам'ятовуючому пристрої мережного криптомодуля, що є засобом кваліфікованого електронного підпису. Запит на формування сертифіката ключа Надавача, що містить відкритий ключ, записується на локальний диск центрального сервера Надавача;
- після генерації особистого ключа Надавача виконується генерація особистих ключів серверів Надавача. Запити на формування сертифікатів ключів серверів Надавача, які містять відкриті ключі, записуються на жорсткі диски відповідних серверів;
- після генерації особистого ключа Надавача та особистих ключів серверів Надавача створюється їх резервні копії. Кожна резервна копія особистого ключа Надавача та особистих ключів серверів Надавача завантажується на захищений носій інформації «Кристал-1» або «Алмаз-1К». Захищені носії інформації з резервними копіями особистого ключа Надавача та особистих ключів серверів Надавача зберігаються в тубусах у безпечному сховищі Надавача;
- керівник Надавача ініціює процес засвідчення чинності відкритого ключа Надавача в центральному засвідчувальному органі відповідно до Регламенту роботи центрального засвідчувального органу;
- після отримання кваліфікованого сертифіката відкритого ключа Надавача від центрального засвідчувального органу, Надавач здійснює їх публікацію на своєму офіційному веб-сайті;
- особистий ключа Надавача вводиться в дію виключно після публікації наказу Міністерства цифрової трансформації України щодо внесення до Довірчого списку нових сертифікатів Надавача та після публікації відповідних сертифікатів на офіційному веб-сайті Надавача;
- поточна пара ключів Надавача стає попередньою, а нова згенерована пара ключів стає поточною.

Після завершення строку чинності кваліфікованого сертифіката попереднього відкритого ключа, та його резервної копії, відповідний особистий ключ та його копія знищуються методом, що не допускає можливості їх відновлення, за участі адміністратора безпеки та адміністратора сертифікації.

Позапланова зміна ключів Надавача виконується у випадку компрометації особистого ключа Надавача або серверів Надавача.

При компрометації особистого ключа Надавача та/або сервера позначок часу (TSP) сертифікати Надавача скасовуються ЦЗО у порядку передбаченому Регламентом роботи ЦЗО та вноситься до списку (реєстру) відкликаних сертифікатів ЦЗО.

Сертифікати Надавача, серверів Надавача та всіх користувачів скасовуються шляхом занесення в список відкликаних сертифікатів.

Сертифікати всіх користувачів, що були сформовані з використанням скомпрометованого ключа Надавача, вважаються не чинними з моменту зміни ЦЗО статусу сертифіката Надавача на скасований або блокований. Інформація про статус сертифіката відкритого ключа Надавача розповсюджується ЦЗО у порядку передбаченому Регламентом роботи ЦЗО.

Усі кваліфіковані сертифікати користувачів, що діяли на момент компрометації ключа Надавача, а також кваліфіковані сертифікати, які були блоковані, повинні бути позапланово замінені.

Під час позапланової заміни Надавач самостійно здійснює виготовлення нових кваліфікованих сертифікатів посадових осіб та користувачів, з використанням їх поточних діючих ключових пар. Термін дії нових позапланово сформованих кваліфікованих сертифікатів визначається терміном дії відповідних старих кваліфікованих сертифікатів, що були скасовані внаслідок заміни.

Надавач, шляхом розміщення відповідної інформації на офіційному інформаційному ресурсі Надавача, оповіщає Користувачів про факт позапланової заміни ключів Надавача та про зміну серійних номерів кваліфікованих сертифікатів Користувачів (формування нових кваліфікованих сертифікатів, підписаних новим ключем Надавача).

Списки відкликаних сертифікатів підписується новим особистим ключем Надавача.

5.7. Компрометація і аварійне відновлення

До об’єктів, процесів та заходів, зазначених в цьому розділі застосовуються вимоги, визначені в пункті 6.4.8 ДСТУ ETSI EN 319 411-1

5.7.1. Процедури обробки інцидентів і компрометації

Порядок дій та реагування на інциденти визначається внутрішніми документами КСЗІ в ІКС Надавача.

Процедури з управління інцидентами повинні передбачати:

- інформування КО про порушення вимог з безпеки та захисту інформації, визначені в абзаці дванадцятому частини четвертої статті 13 Закону України "Про електронну ідентифікацію та електронні довірчі послуги", протягом 24 годин після виявлення порушення;

- інформування користувачів, яким надаються послуги, про порушення безпеки, які спричиняють на них негативний вплив, протягом двох годин після виявлення порушення.

5.7.2. Процедури відновлення, якщо обчислювальні ресурси, програмне забезпечення та/або дані пошкоджені

Процедури оперативного відновлення функціонування ресурсів ІКС Надавача визначаються внутрішніми документами КСЗІ в ІКС Надавача.

5.7.3. Процедури відновлення після компрометації ключа

Якщо є підозра на компрометацію особистого ключа Надавача або його серверів, робота мережних криптомодулів з даними особистими ключами призупиняється, службою захисту інформації Надавача ініціюється службове розслідування.

У разі підтвердження факту компрометації особистого ключа Надавача керівник Надавача та адміністратор безпеки повинні вжити такі заходи:

- зупинити роботу мережних криптомодулів зі скомпрометованими особистими ключами Надавача або його серверів;
- повідомити ЦЗО про компрометацію особистого ключа Надавача;
- скасувати кваліфікований сертифікат Надавача, що відповідає скомпрометованому особистому ключу;
- ініціювати знищення скомпрометованого особистого ключа Надавача у мережному криптомодулі;
- здійснити генерацію нового особистого ключа Надавача та ініціювати формування для нього відповідного кваліфікованого сертифіката Надавача;
- ввести в дію новий особистий ключ Надавача.

5.7.4. Можливості безперервності бізнесу після катастрофи

У випадку непередбаченої ситуації, аварії чи катастрофи, що призвели до виходу з ладу обладнання ІКС, Надавач відновлює свою роботу шляхом заміни або ремонту пошкодженого обладнання та відновлення особистих ключів, даних та інформації з резервних копій.

5.8. Припинення діяльності Надавача

До об’єктів, процесів та заходів, зазначених в цьому розділі, застосовуються вимоги, визначені в пункті 6.4.9 ДСТУ ETSI EN 319 411-1

Припинення діяльності Надавача проводиться відповідно до 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»

5.8.1. Підстави припинення діяльності Надавача

Надавач припиняє свою діяльність з надання кваліфікованих електронних довірчих послуг у разі:

- прийняття ЦЗО рішення про скасування статусу кваліфікованого надавача;
- прийняття Надавачем рішення про припинення надання кваліфікованих електронних довірчих послуг, що зазначені у Довірчому списку;
- припинення діяльності Надавача (припинення юридичної особи), крім випадків правонаступництва, визначених 5.8.4 цієї Політики сертифіката;
- набрання законної сили рішенням суду про скасування статусу кваліфікованого надавача, визнання Надавача банкрутом.

Про рішення щодо припинення надання кваліфікованих електронних довірчих послуг Надавач зобов’язаний повідомити користувачів, ЦЗО та КО не пізніше п’яти робочих днів з дати прийняття такого рішення.

ЦЗО зобов’язаний оприлюднити інформацію про своє рішення щодо припинення діяльності Надавача з надання кваліфікованих електронних довірчих послуг, у тому числі у зв’язку з анулюванням статусу кваліфікованого надавача електронних довірчих послуг, не пізніше наступного робочого дня після прийняття такого рішення шляхом:

- розміщення інформації про таке рішення на своєму офіційному веб-сайті;
- надіслати до Надавача повідомлення про таке рішення із зазначенням підстави його прийняття.

ЦЗО зобов’язаний оприлюднити на своєму офіційному веб-сайті повідомлення про припинення надання кваліфікованих електронних довірчих послуг Надавачем не пізніше наступного робочого дня з дати отримання повідомлення про виникнення підстав для примусового припинення діяльності.

Повідомлення ЦЗО про припинення надання кваліфікованих електронних довірчих послуг Надавачем повинно містити дату публікації.

Надавач припиняє діяльність з надання кваліфікованих електронних довірчих послуг через три місяці з дати оприлюднення ЦЗО на своєму офіційному веб-сайті повідомлення про припинення надання Надавачем кваліфікованих електронних довірчих послуг.

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

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

У разі відмови користувача від продовження отримання послуг за договором про надання електронних довірчих послуг, укладеним з Надавачем, з іншим КНЕДП до закінчення терміну дії відповідного договору, Надавач зобов’язаний повернути кошти такому користувачеві за послуги, які не можуть бути надані в майбутньому, якщо вони були попередньо оплачені користувачем.

Якщо користувач дав згоду на продовження надання послуг за договором про надання електронних довірчих послуг, укладеним з Надавачем, з іншим КНЕДП до закінчення терміну дії відповідного договору, Надавач зобов’язаний оплатити подальше надання кваліфікованих електронних довірчих послуг такому користувачеві за тарифами, встановленими відповідним КНЕДП.

ЦЗО у день, визначений як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг Надавачем, вносить відповідні зміни до Довірчого списку.

У разі припинення надання кваліфікованих довірчих послуг Надавач 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 відкритих ключів, усі сформовані кваліфіковані сертифікати відкритих ключів, а також реєстри сформованих кваліфікованих сертифікатів відкритих ключів).

Передача документованої інформації буде здійснена Надавачем 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 Надавача в день, визначений Надавачем як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, або в день набрання законної сили рішенням відповідного суду.

5.8.2. Повідомлення про припинення діяльності Надавача

Про прийняте рішення про припинення надання кваліфікованих електронних довірчих послуг Надавач 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 Надавачем діяльності з надання кваліфікованих електронних довірчих послуг, в тому числі у зв'язку із скасуванням статусу кваліфікованого надавача електронних довірчих послуг, не пізніше наступного робочого дня після прийняття такого рішення шляхом:

- розміщення інформації про таке рішення на своєму офіційному веб-сайті;
- надіслання до Надавача 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 Надавачем не пізніше наступного робочого дня з дня одержання повідомлення про настання підстав, передбачених пунктом 5.8.1 цієї Політики сертифіката.

Повідомлення ЦЗО про припинення діяльності з надання кваліфікованих електронних довірчих послуг Надавачем повинно містити дату опублікування.

5.8.3. Дата припинення діяльності Надавача

Надавач припиняє свою діяльність з надання кваліфікованих електронних довірчих послуг через три місяці з дня опублікування на своєму офіційному веб-сайті повідомлення про припинення надання кваліфікованих електронних довірчих послуг.

З дня опублікування на своєму офіційному веб-сайті повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг та до дня припинення діяльності з надання кваліфікованих електронних довірчих послуг Надавач зобов'язаний надавати електронні довірчі послуги, крім формування нових кваліфікованих сертифікатів.

ЦЗО у день, визначений як дата припинення діяльності Надавача з надання кваліфікованих електронних довірчих послуг, вносить відповідні зміни до Довірчого списку.

5.8.4. Правонаступництво

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

У разі відмови користувача продовжити обслуговування за договором про надання електронних довірчих послуг, укладеним з Надавачем, що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, в іншого кваліфікованого надавача електронних довірчих послуг до закінчення строку дії відповідного договору, Надавач зобов'язаний повернути такому користувачу кошти за послуги, які не можуть надаватися в подальшому, якщо вони були попередньо оплачені користувачем.

Якщо користувач погодився продовжити обслуговування за договором про надання електронних довірчих послуг, укладеним з Надавачем, що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, в іншого кваліфікованого надавача електронних довірчих послуг до закінчення строку дії відповідного договору, Надавач зобов'язаний оплатити подальше надання кваліфікованих електронних довірчих послуг такому користувачу за тарифами,

встановленими відповідним кваліфікованим надавачем електронних довірчих послуг.

5.8.5. Передача документованої інформації

Надавач у разі припинення діяльності з надання кваліфікованих електронних довірчих послуг зобов'язаний передати до іншого кваліфікованого надавача електронних довірчих послуг, який виявив намір продовжити обслуговування користувачів до закінчення строку дії відповідних договорів про надання кваліфікованих електронних довірчих 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 кваліфікованих електронних довірчих 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 до центрального засвідчувального 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

5.8.6. План припинення діяльності

План припинення діяльності визначає умови, яких повинен дотримуватися Надавач з метою недопущення негативних наслідків у разі припинення ним діяльності з надання кваліфікованих електронних довірчих послуг, а також забезпечення стабільності та довговічності кваліфікованих електронних довірчих послуг.

Надавач 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, центрального засвідчувального органу, персоналу Надавача, відокремлених пунктів реєстрації, суб’єктів, які довіряють Надавачу та контрагентів про припинення діяльності з надання кваліфікованих електронних довірчих послуг;

- домовленості та угоди з третіми сторонами для продовження виконання зобов'язань у разі припинення Надавачем діяльності з надання кваліфікованих електронних довірчих послуг (передача обслуговування користувачів до іншого кваліфікованого надавача).

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

Крім того, застосовуються такі особливі вимоги:

6.1. Генерація та встановлення пари ключів

6.1.1. Генерація пари ключів

6.1.1.1.Генерація пари ключів Надавача

Генерація особистого ключа Надавача виконується у криптографічному модулі на центральному сервері ІКС КНЕДП «MASTERKEY», який знаходиться у спеціальному приміщенні, двома особами – адміністратором сертифікації під контролем адміністратора безпеки.

Порядок генерації особистого ключа Надавача визначено в пункті 5.6 цієї Політики сертифіката.

6.1.1.2.Генерація пари ключів користувача

Особистий та відкритий ключі користувача при отриманні ним електронних довірчих послуг можуть бути згенеровані користувачем на власній робочій станції або на станції генерації Надавача та його відокремлених пунктах реєстрації.

Генерація відкритого та особистого ключів користувача здійснюється з застосуванням засобів кваліфікованого електронного підпису, які мають документи про відповідність або позитивний експертний висновок за результатами їх державної експертизи у сфері криптографічного захисту інформації.

В процесі генерації та впродовж використання особистий ключ користувача не покидає меж захищеного носія особистого ключа та захищається паролем і залишається у користувача, який несе відповідальність за забезпечення його конфіденційності та цілісності.

Захищеними носіями особистих ключів є носії, що відповідають вимогам статті 19 Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Засіб кваліфікованого електронного підпису та печатки за допомогою відповідного особистого ключа створює самопідписані запити на формування кваліфікованих сертифікатів підпису та шифрування, які містять відкриті ключі користувача та додаткову інформацію для формування кваліфікованих сертифікатів у Надавача.

При виборі паролю захисту особистого ключа необхідно враховувати наступні рекомендації:

- довжина паролю повинна містити не менше 8 символів;
- символи паролю не повинні повторюватись;
- пароль не повинен містити підряд більше ніж 2 символи з розкладки клавіатури;
- в паролі використовувати наступні символи - 'a-z', 'A-Z', '0-9', '+', '-'.

Довжина паролів захисту особистого ключа для захищених носіїв ключової інформації повинна містити кількість символів, передбачену технічною документацією на такі носії.

Після генерації особистого ключа на захищеному носії особистого ключа виводиться вміст простого запиту на формування сертифікату з відкритим ключем для державних алгоритмів та протоколів. Запити на формування кваліфікованих сертифікатів підпису та шифрування зберігаються Користувачем у форматах: "ПІБ EU-XXXXXXXX.p10" та "ПІБ EU-KEP-XXXXXXXX.p10" відповідно (для електронної печатки замість "ПІБ" зазначається "електронна печатка та ЄДРПОУ юридичної особи"). Розширення файлу запиту (.p10) повинно залишатися без змін.

Запити на формування кваліфікованих сертифікатів підпису та шифрування в онлайн сервісі «OLS» Надавача має наступний вигляд:

EU-XXXXXXXX.p10 = "_request_sign_yyyymmddxxxxxx

".p10" - унікальне ім'я файлу запиту для формування кваліфікованого сертифіката підпису, що створюється за замовчуванням;

"EU-KEP-XXXXXXXX.p10 = "_request_crypt_yyyymmddxxxxxx.p10" - унікальне ім'я файлу запиту для формування кваліфікованого сертифіката шифрування, що створюється за замовчуванням.

Запити на формування кваліфікованих сертифікатів підпису та шифрування ІКС Надавача має наступний вигляд:

"ім'я файлу для запису запиту з відкритим ключем - "EU-XXXXXXXX.p10".

"ім'я файлу для запису запиту з відкритим ключем протоколу розподілу - "EU-KEP-XXXXXXXX.p10"

Приклад:

ПІБ EU-6E50VH92.p10;

ПІБ EU-KEP-3R15GT23.p10, де:

- "ПІБ" - прізвище, ім'я, по батькові Користувача;
- "EU-6E50VH92.p10" - унікальне ім'я файлу запиту для формування кваліфікованого сертифіката підпису, що створюється за замовчуванням;
- "EU-KEP-3R15GT23.p10" - унікальне ім'я файлу запиту для формування кваліфікованого сертифіката шифрування, що створюється за замовчуванням.

Надання сформованих користувачем запитів здійснюється на носії інформації особисто користувачем або його уповноваженою особою після процедури ідентифікації та реєстрації користувача.

Особистий ключ користувача генерується на захищений носій особистого ключа, а сформовані запити на формування кваліфікованих сертифікатів передаються на службовому носії інформації на робочу станцію адміністратора реєстрації.

Особисті ключі користувачів та паролі захисту до них у Надавача не зберігаються.

6.1.2. Доставка особистого ключа користувачу

Отримання користувачем особистого ключа відбувається у момент генерації особистого ключа на власній робочій станції або на станції генерації ВПР Надавача.

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 та формується під час генерації особистого та відкритого ключів засобами кваліфікованого електронного підпису чи печатки.

6.1.4. Доставка відкритого ключа надавача суб'єктам, які довіряють надавачу

Кваліфіковані сертифікати Надавача та центрального засвідчувального органу, публікуються на офіційному веб-сайті Надавача.

Доступ до актуального кваліфікованого сертифіката Надавач забезпечено на офіційному веб-сайті ЦЗО

6.1.5. Розміри (параметри) ключів

В ІКС Надавача використовуються особисті та відповідні їм відкриті ключі з параметрами, що відповідають таким вимогам:

- алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 257 біт або 431 біт, що відповідає ДСТУ 4145-2002.

6.1.6. Генерація параметрів відкритого ключа

Під час генерації відкритого ключа використовується апаратний генератор випадкових чисел. Ключі генеруються та зберігаються в апаратному мережевому криптомодулі.

6.1.7. Основні цілі використання особистого ключа надавачем

Особисті ключі Надавача та серверів OCSP, CMP Надавача забезпечують функціонування ІКС Надавача.

Надавач використовує ключі Надавача для підпису сертифікатів користувачів, сертифікатів серверів OCSP, CMP Надавача, списків 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 використовуються засоби кваліфікованого електронного підпису чи печатки, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами державної експертизи або сертифікації таких засобів, а також на файлових носіях у вигляді файлів з розширенням *.dat

Для зберігання особистих ключів Надавача та серверів ІКС Надавача 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 державної експертизи або сертифікації таких засобів.

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

Доступ до особистого ключа Надавача мають тільки уповноважені посадові особи Надавача під контролем адміністратора безпеки.

Управління особистими ключами Надавача здійснюється посадовими особами тільки після їх автентифікації в мережному криптомодулі.

6.2.3. Управління особистим ключем підписувача

Надавач не зберігає особисті ключі користувачів в мережних криптомодулях які відносяться до Надавача.

6.2.4. Резервне копіювання особистого ключа

Резервне копіювання особистих ключів Надавача та його серверів здійснюються адміністратором сертифікації під контролем адміністратора безпеки.

Під час резервного копіювання особистих ключів Надавача та серверів ІКС Надавача створюється не менше двох резервних копій особистого ключа з криптомодуля. Кожна резервна копія особистого ключа записується на зовнішній засіб кваліфікованого електронного підпису чи печатки, який є апаратно-програмним або апаратним пристроєм у захищеному вигляді, що забезпечує їх цілісність та конфіденційність.

6.2.5. Архівація особистого ключа

Особисті ключі Надавача та його серверів знищуються відповідальними посадовими особами Надавача після закінчення строку дії відповідних кваліфікованих сертифікатів.

6.2.6. Відновлення особистого ключа

Відновлення особистих ключів Надавача та серверів ІКС Надавача здійснюється з резервних копій.

6.2.7. Зберігання особистого ключа в криптографічному модулі

Особисті ключі Надавача та серверів ІКС Надавача зберігаються та захищаються від несанкціонованого доступу в мережних криптомодулях, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами державної експертизи або сертифікації таких засобів.

6.2.8. Активація особистих ключів

Введення в дію особистого ключа Надавача та серверів Надавача (OCSP, CMP, TSP) виконується на сервері ІКС КНЕДП «MASTERKEY» у службовому приміщенні Надавача.

6.2.9. Деактивація особистих ключів

Процедура деактивації особистих ключів Надавач шляхом їх знищення визначена в пункті 6.2.10 цієї Політики сертифіката.

6.2.10. Знищення особистих ключів

Після завершення строку чинності кваліфікованого сертифіката Надавача та серверів Надавача (OCSP, CMP, TSP), відповідний особистий ключ та всі його резервні копії знищуються.

Знищення особистих ключів Надавача та серверів Надавача (OCSP, CMP, TSP) здійснюється згідно з експлуатаційною документацією на відповідні засоби кваліфікованого електронного підпису чи печатки у яких вони зберігалися та використовувалися.

Процедури знищення особистих ключів повинні забезпечувати неможливість відновлення ключів після знищення.

6.2.11. Можливості мережного криптографічного модуля

Мережний криптомодуль підтримує процедури, які охоплюють безпечне функціонування Надавача (генерація ключів, резервне копіювання, зберігання, знищення).

Усі мережні криптографічні модулі, що містять копії особистого ключа Надавача та його серверів, фізично захищені від несанкціонованого доступу.

Усі операції підписання за допомогою особистого ключа Надавача виконуються в мережевому криптомодулі Надавача.

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 Надавача постійно.

6.3.2. Строки дії сертифіката та строки використання пари ключів

Строки дії особистих ключів Надавача відповідають строкам чинності кваліфікованих сертифікатів відповідних їм відкритих ключів і становлять:

- для особистих ключів Надавача та його серверів - 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

Особисті ключі, які зберігаються на засобах кваліфікованого електронного підпису чи печатки, повинні захищатися паролями, що складаються не менше ніж з 8 символів, які містять великі та малі латинські літери, цифри та символи.

6.4.3. Інші аспекти даних активації

Жодних умов.

6.5. Контроль комп'ютерної безпеки

6.5.1. Спеціальні технічні вимоги до комп’ютерної безпеки

Надавач забезпечує захист інформаційних ресурсів від зовнішніх загроз, атак та несанкціонованого витоку інформації шляхом впровадження в ІКС комплексної системи захисту інформації (КСЗІ), яка має атестат відповідності за результатами проведення державної експертизи в сфері технічного захисту інформації.

Надавач забезпечує:

- конфіденційність та цілісність інформації, яка зберігається й обробляється в компонентах ІКС Надавача, а також передається між ними;
- конфіденційність особистих ключів, що використовуються Надавачем та його користувачами;
- конфіденційність технологічної інформації, яка забезпечує функціонування ІКС Надавача;
- доступ до інформації та ресурсів ІКС Надавача користувачам згідно з правилами, встановленими політикою безпеки Надавача;
- спостереженість за діями користувачів шляхом впровадження механізмів і процедур контролю, реєстрації та проведення аудиту зареєстрованих подій.

6.5.2. Рейтинг комп'ютерної безпеки

Комплексна система захисту інформації в ІКС Надавача має чинний атестат відповідності за результатами проведення державної експертизи в сфері технічного захисту інформації.

6.6. Контроль безпеки життєвого циклу

6.6.1. Контроль розробки системи

При розробці та впровадженні ІКС Надавача повинні бути враховані існуючі тенденції розвитку захищених інформаційних технологій, відомі розробки відповідних засобів захисту інформації, вимоги нормативної бази з технічного захисту інформації.

Для здійснення захисту інформації на всіх стадіях життєвого циклу ІКС Надавача повинна передбачати застосування наступних заходів та засобів захисту інформації:

- організаційно-правові заходи, які реалізуються поза ІКС Надавача;
- інженерно-технічні заходи, що реалізуються поза ІКС Надавача;
- апаратні, програмно-апаратні та програмні засоби захисту від несанкціонованого доступу до інформації, яка обробляється і зберігається в ІКС Надавача.

Апаратне забезпечення комплексу засобів захисту Надавач отримує безпосередньо від розробника, або від організацій, що мають відповідні ліцензії на впровадження комплексу засобів захисту комплексу технічних рішень.

6.6.2. Засоби керування безпекою

Контроль за дотриманням вимог з безпеки в ІКС Надавача здійснюється позаштатним підрозділом служби захисту інформації Надавача, на яку покладається забезпечення захисту інформації в ІКС.

Підтримка функціонування та обслуговування системи здійснюється адміністраторами згідно їх посадових обов’язків та документації КСЗІ.

6.6.3. Контроль безпеки протягом життєвого циклу

Надавач гарантує, що обладнання та робочі станції адміністраторів ІКС Надавача своєчасно модернізуються та мають останні оновлення безпеки.

6.7. Контроль безпеки мережі

Надавач виконує всі технічні дії із забезпечення захисту в ІКС КНЕДП «MASTERKEY» відповідно до внутрішньої документації КСЗІ.

6.8. Електронні позначки часу

6.8.1. Формування кваліфікованої електронної позначки часу

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 Надавача.

Формування кваліфікованої електронної позначки часу здійснюється Надавачем за запитом користувача.

Під час формування кваліфікованої електронної позначки часу користувач та Надавач за допомогою засобу кваліфікованого електронного підпису чи печатки вчиняють такі дії:

- користувач обчислює геш-значення електронних даних, на які необхідно сформувати кваліфіковану електронну позначку часу;

- користувач формує запит на формування кваліфікованої електронної позначки часу, який містить:

    - обчислене геш-значення;
    - об’єктний ідентифікатор (OID) політики формування позначки часу (необов’язково);
    - ідентифікатор алгоритму гешування, що використовувався;
    - унікальний ідентифікатор запиту (необов’язково);
    - необов’язкові розширення;

- користувач передає сформований запит до Надавача;
- Надавач перевіряє правильність формату запиту та здійснює його обробку, формує кваліфіковану електронну позначку часу та відповідь, що містить кваліфіковану електронну позначку часу, чи відповідь з інформацією про відмову у формуванні кваліфікованої електронної позначки часу;
- Надавач надсилає користувачеві відповідь, що містить кваліфіковану електронну позначку часу, в якій зазначені такі дані:

    - об’єктний ідентифікатор (OID) політики формування кваліфікованої електронної позначки часу, що була використана;
    - геш-значення електронних даних, для яких було сформовано кваліфіковану електронну позначку часу;
    - серійний номер кваліфікованої електронної позначки часу;
    - час формування кваліфікованої електронної позначки часу;
    - додаткову інформацію про кваліфіковану електронну позначку часу;
    - кваліфікований електронний підпис чи печатку Надавача, накладені на кваліфіковану електронну позначку часу;

- користувач після отримання відповіді від Надавача вчиняє такі дії:

    - перевіряє результат обробки запиту;
    - перевіряє відповідність імені чи найменування суб’єкта, що наклав кваліфікований електронний підпис чи печатку на кваліфіковану електронну позначку часу, найменуванню Надавача;
    - перевіряє відповідність призначення сертифіката Надавача (для формування позначки часу);
    - перевіряє чинність сертифіката Надавача;
    - перевіряє кваліфікований електронний підпис чи печатку, що був накладений на кваліфіковану електронну позначку часу;
    - перевіряє відповідність електронних даних та даних, для яких була сформована кваліфікована електронна позначка часу (шляхом порівняння обчисленого геш-значення електронних даних та геш-значення, що записане у кваліфікованій електронній позначці часу);

- додає кваліфіковану електронну позначку часу до електронних даних.

6.8.2. Перевірка кваліфікованої електронної позначки часу

Кваліфікована електронна позначка часу повинна забезпечувати:

- зв’язок дати і часу з електронними даними в такий спосіб, що цілком виключає можливість непомітної зміни електронних даних;
- точність часу в програмно-технічному комплексі Надавача, що синхронізується із Всесвітнім координованим часом (UTC) з точністю до секунди.

Перевірка кваліфікованої електронної позначки часу може проводитися будь-якою особою 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:

- отримує з кваліфікованої електронної позначки часу інформацію, що містить ідентифікаційні дані особи, які дають змогу однозначно встановити Надавача;
- перевіряє кваліфікований електронний підпис чи печатку, накладений на кваліфіковану електронну позначку часу за допомогою чинного (на момент формування кваліфікованої електронної позначки часу) сертифіката Надавача;
- перевіряє відповідність кваліфікованої електронної позначки часу та електронних даних,до яких вона додана (шляхом порівняння обчисленого геш-значення електронних даних та геш-значення, що записане у кваліфікованій електронній позначці часу).

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 Надавача;
- використання скасованого або блокованого сертифіката Надавача на момент формування кваліфікованої електронної позначки часу.

6.8.4. Отримання кваліфікованої електронної позначки часу надавачем

Надавач 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 Надавача 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 Надавачем 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

7.1. Профілі сертифікатів

Кваліфіковані сертифікати, що формуються Надавачем повинні відповідати вимогам таких стандартів:

- ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння». З функцією ґешування за ГОСТ 34.311-95 «Інформаційна технологія. Криптографічний захист інформації. Функція ґешування» або за ДСТУ 7564-2014 «Інформаційні технології. Криптографічний захист інформації. Функція ґешування»;
- 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».

Поля та формат інформації, що міститься в кваліфікованому сертифікаті наведено у Таблиці 3:

Таблиця 3

Найменування	Значення
Версія	Версія 3 (стандарт X.509)
Серійний Номер	Унікальний номер сертифіката
Алгоритм підпису	Визначає криптографічний алгоритм, який використовується для підпису кваліфікованого сертифіката
Постачальник	Назва надавача, що формує кваліфікований сертифікат
Дійсний з	Дата початку дії кваліфікованого сертифіката
Дійсний до	Дата закінчення строку дії кваліфікованого сертифіката
Тема	Інформація про отримувача кваліфікованого сертифіката
Відкритий ключ	Відкритий ключ, що відповідає особистому ключу кваліфікованого сертифіката
Підпис	Кваліфікований електронний підпис надавача, що надає послугу створення, перевірки та підтвердження кваліфікованого електронного

	підпису чи печатки

7.2. Профілі списку відкликаних сертифікатів (CRL)

Списки відкликаних сертифікатів (CRL), що формуються Надавачем 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»;
- RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

Поля та формат інформації, що міститься в CRL, опубліковані на офіційному веб-сайті Надавача наведено у Таблиці 4:

Таблиця 4

Найменування	Значення
Версія	Версія 2
Постачальник	Назва надавача, що формує CRL
Початок дії	Поточна дата випуску CRL
Наступне оновлення	Дата наступного оновлення CRL
Алгоритм підпису	Алгоритм, що використовується для підписання CRL
Скасовані сертифікати	У цьому полі міститься інформація про скасовані кваліфіковані сертифікати, зокрема: - серійний номер скасованого кваліфікованого сертифіката; - дата та час, коли кваліфікований сертифікат було скасовано
Номер списку	Реєстраційний номер списку CRL
Підпис	Значення цифрового підпису від надавача

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.

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

8.1. Частота або обставини оцінювання

Не допускається надання кваліфікованих електронних довірчих послуг без чинних документів, визначених законодавством, що підтверджують відповідність ІКС Надавача 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.

Надавач 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 Надавачем 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 надавача за рахунок такого надавача для підтвердження того, що він та електронні довірчі послуги, які він надає, відповідають вимогам у сфері електронних довірчих послуг.

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

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 Надавача.

Перевірка здійснюється відповідно до рішення КО.

Рішення щодо проведення перевірки повинно містити:

- найменування Адміністрації Держспецзв'язку;
- найменування надавача;
- місцезнаходження надавача;
- підставу для проведення перевірки;
- предмет перевірки;
- дати початку та закінчення перевірки;
- 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 надавачів та послуг, що ними надаються.

ООВ повинен дотримуватися положень, визначених у стандарті ДСТУ ETSI EN 319 4031 (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.

8.3. 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 Надавача;
- ознайомлювати керівника Надавача чи уповноваженого ним представника з результатами перевірки;
- надавати Надавачу 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 Надавачем.

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.

8.5. 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 Надавача усунення порушень вимог законодавства у сфері електронних довірчих послуг у встановлений приписом строк;
2) приймає рішення про блокування кваліфікованого сертифіката Надавача, якщо під час перевірки виникла підозра компрометації особистого ключа;
3) приймає рішення про скасування кваліфікованого сертифіката Надавача, якщо під час перевірки виявлено факт компрометації особистого ключа;
4) надсилає до ЦЗО подання про відкликання статусу кваліфікованого надавача електронних довірчих послуг або послуги, яку надає Надавач, у Довірчому списку в разі:

- надання кваліфікованих електронних довірчих послуг надавачем без чинних документів, визначених законодавством, що підтверджують відповідність 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;

- надання кваліфікованих електронних довірчих послуг за відсутності у Надавача 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 надавачем своїх зобов'язань;
- порушення вимог до умов експлуатації СУІБ або КСЗІ ІКС Надавача;
- надання кваліфікованих електронних довірчих послуг Надавача 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 Надавачем для внесення відомостей про нього до Довірчого списку;
- не усунення виявлених під час перевірки порушень у встановлений приписом строк;
- блокування або скасування кваліфікованого сертифіката Надавача.

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 Надавача або послуги, яку надає Надавач, у Довірчому списку в разі надання кваліфікованих

електронних довірчих послуг Надавачем без чинних документів, визначених законодавством, що підтверджують відповідність 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.

8.6. Повідомлення результатів

8.6.1. Оформлення результатів державного контролю

Результати проведення перевірки надавача 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 Надавача;
- реквізити посвідчення на проведення перевірки;
- дати початку і закінчення перевірки;
- адреса приміщень Надавача, 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 Надавача, пов'язану з наданням електронних довірчих послуг;
- виявлені під час перевірки порушення і недоліки (за наявності) та пояснення Надавача 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 Надавача 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 Надавача 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 Надавача 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 Надавача чи уповноваженим ним представником.

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

Якщо керівник Надавача 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 Надавача 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 надавачу, а другий примірник з підписом керівника надавача 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 Надавача 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 Надавача повинен вжити заходів до усунення недоліків та порушень, зазначених у приписі про усунення порушень, протягом визначеного у приписі строку.

Надавач 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 Надавача (найменування, ідентифікаційні дані та контактна інформація);
- сфера оцінки відповідності;
- перелік кваліфікованих електронних довірчих послуг, які має намір надавати КНЕДП;
- найменування ІКС Надавача;
- 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 Надавач повинний 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.

8.7. **Самоперевірки**

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

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

9.1. Збори

9.1.1. Плата за видачу або поновлення сертифіката

За формування кваліфікованого сертифіката сплачується плата, вартість якої визначається згідно з тарифними планами на надання кваліфікованих

електронних довірчих послуг КНЕДП «MASTERKEY», опублікованими на офіційному веб-сайті Надавача.

Поновлення заблокованих кваліфікованих сертифікатів здійснюється на безоплатній основі.

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

Надавач може надавати користувачам додаткові послуги за плату, серед яких:

- надання засобів кваліфікованого електронного підпису чи печатки користувачам;
- виїзна генерація пари ключів користувача.

9.1.5. Політика відшкодування

Надавач не відшкодовує сплачені рахунки, послуги по яким надані.

9.2. Фінансова відповідальність

Діяльність Надавача відповідає вимогам частини п'ятої статті 16 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» щодо надання кваліфікованих електронних довірчих послуг за умови внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам. 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 Надавач обробляє конфіденційну інформацію, яка не оприлюднюється для загального ознайомлення. Захист конфіденційної інформації здійснюється відповідно чинного законодавства.

9.3.2. Інформація, що не належить до конфіденційної

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

9.3.3. Відповідальність за захист конфіденційної інформації

Надавач здійснює захист конфіденційної інформації та несе відповідальність згідно з вимогами чинного законодавства.

9.4. Конфіденційність персональних даних

9.4.1. Концепція захисту персональних даних

Концепція захисту персональних даних Надавач у процесі надання кваліфікованих електронних довірчих послуг здійснює:

- 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

Надавач гарантує дотримання вимог законодавства про захист персональних даних та несе відповідальність згідно з вимогами чинного законодавства.

9.4.5. Інформація та згода на використання персональних даних

Відповідно до Закону України "Про захист персональних даних" Надавач надає кваліфіковані довірчі 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

Надавач надає доступ до персональних даних користувачів лише у випадках, передбачених Законом України "Про захист персональних даних".

Керівник Надавача та персонал Надавача дотримуються вимог законодавства України в сфері захисту персональних даних та підписують договір про конфіденційність та нерозголошення інформації.

9.5. Права інтелектуальної власності

Питання прав інтелектуальної власності Надавача врегульовані відповідно до вимог чинного законодавства України.

9.6. Зобов’язання та гарантії

9.6.1. Зобов’язання та гарантії Надавача

Надавач надає кваліфіковані електронні довірчі послуги з дотриманням вимог законодавства у сфері електронних довірчих послуг, цієї Політики сертифіката та відповідних Положень сертифікаційних практик.

9.6.2. Зобов’язання та гарантії відокремлених пунктів реєстрації

На підставі договору, укладеного з Надавачем (ТОВ «Арт-мастер»), реєстрацію користувачів здійснюють відокремлені пункти реєстрації Надавача, які виконують свої функції згідно з цією Політикою сертифіката та відповідними Положеннями сертифікаційних практик.

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

9.6.3. Зобов’язання та гарантії користувачів

Користувачі зобов'язані:

- забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;
- невідкладно повідомляти Надавачу про підозру або факт компрометації особистого ключа;
- надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;
- своєчасно здійснювати оплату за електронні довірчі послуги, якщо така оплата передбачена договором між Надавачем та користувачем;
- своєчасно надавати Надавачу 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 в кваліфікованому сертифікаті;
- 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.

До договору про надання електронних довірчих послуг можуть бути включені додаткові умови. Зміст договору про надання електронних довірчих послуг публікується на веб-сайті Надавача.

9.6.4. Зобов’язання та гарантії суб’єктів, які довіряють Надавачу

Суб’єкт, який довіряє Надавачу, повинен перевірити чинність кваліфікованого сертифіката сформованого Надавачем, перед використанням кваліфікованого сертифіката.

9.6.5. Зобов’язання та гарантії інших учасників

ЦЗО, перш ніж прийняти рішення про внесення Надавача до Довірчого списку та надання йому кваліфікованого статусу, пересвідчився щодо наявності в Надавача:

- документа, що підтверджує відповідність системи захисту інформації Надавача вимогам положень статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах»;

- документів, які підтверджують право власності та право користування Надавача нежилими приміщеннями, які використовуються для розміщення всіх складових програмно-технічного комплексу, що забезпечують надання кваліфікованих електронних довірчих послуг;
- належного персоналу Надавача;
- документів, які підтверджують освітньо-кваліфікаційний рівень та трирічний стаж роботи за фахом персоналу Надавача;
- документів, які підтверджують право власності або право користування засобами кваліфікованого електронного підпису чи печатки, які використовуються Надавачем для надання кваліфікованих електронних довірчих послуг;
- документів, що підтверджують внесення коштів на поточний рахунок Надавача із спеціальним режимом використання у банку, або договору страхування відповідальності, для забезпечення відшкодування збитків, які можуть бути заподіяні користувачам унаслідок неналежного виконання Надавачем своїх обов'язків;
- цієї Політики сертифіката та відповідних Положень сертифікаційних практик;
- відомостей про відокремлені пункти реєстрації та їхніх працівників, обов'язки яких будуть безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг.

9.7. Відмова від гарантій

Надавач не надає жодних гарантій щодо послуг, які ним надаються, крім тих, які були чітко визначені в пункті 9.6.1 цієї Політики сертифіката.

9.8. Обмеження відповідальності

У разі якщо Надавач належним чином заздалегідь повідомить користувачів про обмеження щодо використання електронних довірчих послуг, які він надає, за умови що такі обмеження є зрозумілими для користувачів, він не несе відповідальності за шкоду, завдану внаслідок використання електронних довірчих 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 Надавачем 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 Надавача.

9.11. Індивідуальні повідомлення та комунікації з учасниками інфраструктури відкритих ключів

Надавач здійснює комунікацію з учасниками інфраструктури відкритих ключів шляхом:

- розміщення повідомлень та оголошень на офіційному веб-сайті Надавача;
- 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 або смс-інформування на номер телефону користувача.

9.12. Зміни

Внесення змін до цієї Політики сертифіката здійснюється Надавачем у разі:

- змін вимог, процесів та процедур, описаних в цій Політиці сертифіката;
- змін в законодавстві;
- змін у вимогах до надавачів щодо надання послуг.

Нові версії цієї Політики сертифіката після внесення змін до неї публікуються на офіційному веб-сайті Надавача.

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, Надавач 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 Надавач повинен дотримуватися вимог:

- Закону України «Про електронну ідентифікацію та електронні довірчі послуги»;
- Закону України «Про захист інформації в інформаційно-комунікаційних системах»;
- Закону України «Про захист персональних даних»;
- постанови Кабінету Міністрів України від 27 січня 2010 р. № 55 «Про впорядкування транслітерації українського алфавіту латиницею»;
- постанова Кабінету Міністрів України від 01 серпня 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 10 грудня 2024 р. № 1408 «Деякі питання зберігання документованої інформації та її передавання до центрального засвідчувального органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг»;
- постанови Кабінету Міністрів України від 28.06.2024 р. № 764 «Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг»;
- постанови Кабінету Міністрів України від 13 вересня 2024 р. № 1062 «Про затвердження Порядку проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг»;
- 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 12 грудня 2023 р. № 1298 «Про затвердження вимог до форматів удосконалених електронних підписів та печаток, які використовуються для надання електронних публічних послуг, та вимог до створення та перевірки удосконалених електронних підписів та печаток, що базуються на кваліфікованих сертифікатах відкритих ключів»;
- наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 1 лютого 2019 р. № 316/5/57 «Про позначку кваліфікованого сертифіката відкритого ключа», зареєстрованого в Міністерстві юстиції України 5 лютого 2019 р. за № 123/33094;

- наказу Міністерства цифрової трансформації України від 17 листопада 2023 р. № 149 «Про затвердження Порядку ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів, які сформовані центральним засвідчувальним органом», зареєстрованого в Міністерстві юстиції України 05 грудня 2023 р. за № 2110/41166;
- наказу Міністерства цифрової трансформації України від 25 серпня 2020 р. № 125 «Про Вимог до формату реєстрів сформованих кваліфікованих сертифікатів відкритих ключів, а також носіїв інформації та порядку запису на них документів в електронній формі», зареєстрованого в Міністерстві юстиції України 6 листопада 2020 р. за № 1086/35369;
- наказу Міністерства цифрової трансформації України від 06.04.2024 р. №54 «Про затвердження форми плану припинення діяльності з надання кваліфікованих електронних довірчих послуг», зареєстрованого в Міністерстві юстиції України 23 квітня 2024 р. за № 588/41933;
- наказу Міністерства цифрової трансформації України від 28 лютого 2024 р. № 33 «Про затвердження Регламенту роботи центрального засвідчувального органу», зареєстрованого в Міністерстві юстиції України 15 березня 2024 р. за № 393/41738.