ПОГОДЖЕНО

Перший заступник Міністра цифрової трансформації України

_____ Олексій ВИСКУБ

«___»_____ 2025 р.

ЗАТВЕРДЖУЮ

Директор ТОВ «Центр сертифікації ключів «Україна»

_____ Валерій КОХНО

«___»_____ 2025 р.

РЕГЛАМЕНТ
РОБОТИ КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ ТОВАРИСТВА З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ «УКРАЇНА»

На 129 аркушах

Київ 2025

Зміст

ВСТУП

Перелік умовних позначень та скорочень

Умовні позначення та скорочення	Опис
Надавач	Кваліфікований надавач електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна»
ВПР	Відокремлений пункт реєстрації
Договір	Договір про надання кваліфікованих електронних довірчих послуг
ЄДДР	Єдиний державний демографічний реєстр
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань
ЄДРПОУ	Єдиний державний реєстр підприємств та організацій України
ЗКЕП	Засіб кваліфікованого електронного підпису чи печатки
ІКС	Інформаційно-комунікаційна система
КЕП	Кваліфікований електронний підпис
КЗІ	Криптографічний захист інформації
КНЕДП	Кваліфікований надавач електронних довірчих послуг
КСЗІ	Комплексна система захисту інформації
ОС	Операційна система
ПЗ	Програмне забезпечення
ПТК	Програмно-технічний комплекс - апаратно-програмні та програмні засоби, що забезпечують виконання функцій КНЕДП
Регламент	Регламент роботи кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна»
РНОКПП	Реєстраційний номер облікової картки платника податків
ЦЗО	Центральний засвідчувальний орган
OCSP	Online Certificate Status Protocol

TSP	Time Stamp Protocol

Терміни та визначення

У цьому Регламенті терміни та визначення застосовуються у значеннях, наведених у Цивільному кодексі України, Законі України від 05 жовтня 2017 року № 2155-VIII "Про електронну ідентифікацію та електронні довірчі послуги", постанові Кабінету міністрів України від 28 червня 2024 року № 764 «Деякі питання електронної ідентифікації та електронних довірчих послуг», інших нормативно-правових актах з питань криптографічного та технічного захисту інформації.

Статус Регламенту

Цей Регламент визначає організаційно-методологічні, технічні та технологічні умови діяльності Надавача під час надання кваліфікованих електронних довірчих послуг, включаючи політику сертифіката та положення сертифікаційних практик.

Регламент розроблений відповідно до:

- Закону України від 05 жовтня 2017 року № 2155-VIII «Про електронну ідентифікацію та електронні довірчі послуги»;
- Закону України від 22 травня 2003 року № 851 - IV «Про електронні документи та електронний документообіг»;
- Закону України від 15 травня 2003 року № 755 - IV «Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань»;
- постанови Кабінету Міністрів України від 28 червня 2024 року № 764 «Деякі питання електронної ідентифікації та електронних довірчих послуг»;
- інших нормативно-правових актів у сфері надання електронних довірчих послуг.

Норми цього Регламенту поширюються на:

- працівників Надавача;
- заявників;
- підписувачів;
- створювачів електронної печатки.

Вимоги Регламенту є обов’язковими до виконання працівниками Надавача.

Визнання вимог Регламенту заявниками, підписувачами та створювачами електронних печаток є обов’язковою умовою для укладання з ними договору про надання електронних довірчих послуг.

Регламент та зміни до нього публікуються на офіційному веб-сайті Надавача.

Внесення змін та доповнень до Регламенту

Погодження, внесення змін та доповнень до цього Регламенту здійснюється Надавачем згідно чинного законодавства України.

Про внесення змін та доповнень до цього Регламенту Надавач повідомляє заявників, підписувачів, створювачів електронних печаток та інших зацікавлених осіб шляхом розміщення зазначених змін та доповнень на офіційному веб-сайті Надавача.

Всі зміни та доповнення, внесені Надавачем до цього Регламенту, що не пов'язані зі зміною законодавства, набувають чинності через 10 календарних днів з дня розміщення зазначених змін і доповнень на офіційному веб-сайті Надавача.

Всі зміни та доповнення, внесені Надавачем до цього Регламенту у зв'язку зі зміною законодавства, набувають чинності одночасно зі вступом в силу відповідних нормативно-правових актів, але не раніше моменту опублікування змін до цього Регламенту на офіційному веб-сайті Надавача.

1.ЗАГАЛЬНІ ВІДОМОСТІ ПРО НАДАВАЧА

Повні найменування Надавача: товариство з обмеженою відповідальністю «Центр сертифікації ключів «Україна», Limited Liability Company «Key Certification Center «Ukraine».

Скорочені найменування Надавача: ТОВ «Центр сертифікації ключів «Україна», «Key Certification Center «Ukraine» LLC.

Юридична та фактична адреса Надавача: Україна, 03142, м. Київ, вул. Ірпінська, 1.

Телефон: +38 (044) 206-72-31.

Код ЄДРПОУ: 36865753.

Електронна адреса веб-сайту Надавача: **uakey.com.ua**

Адреса електронної пошти Надавача: **info@uakey.com.ua**

Графік роботи Надавача розміщується на веб-сайті Надавача.

Для надання кваліфікованих електронних довірчих послуг на певній території Надавач може створювати представництва (відокремлені пункти реєстрації) або відряджати посадових осіб (адміністраторів реєстрації) до певного регіону.

Представництвами Надавача є відокремлені пункти реєстрації, що представлені окремими підрозділами або філіями Надавача, або юридичні чи фізичні особи, які на підставі договору з ТОВ «Центр сертифікації ключів «Україна» здійснюють реєстрацію підписувачів з дотриманням вимог законодавства у сферах електронної ідентифікації, електронних довірчих послуг та захисту інформації. Перелік представництв публікується на веб-сайті Надавача.

Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені ТОВ «Центр сертифікації ключів «Україна» або від імені представництва.

2.ПЕРЕЛІК КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

Надавач забезпечує надання таких кваліфікованих електронних довірчих послуг:

- кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки;
- кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;
- кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованої електронної позначки часу.

3.ПЕРЕЛІК ПОСАД ТА ФУНКЦІЇ ПЕРСОНАЛУ НАДАВАЧА

Персоналом Надавача, посадові обов'язки якого безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг у головному офісі Надавача, є працівники, на яких покладено функціональні обов'язки:

- керівника Надавача;
- адміністратора реєстрації;
- адміністратора сертифікації;
- адміністратора безпеки;
- системного адміністратора;
- аудитора системи.

Детальний опис обов'язків персоналу Надавача визначено в пункті 5.3.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Детальний опис обов'язків посадових осіб відокремлених пунктів реєстрації Надавача визначено в пункті 5.3.5. Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

4.ПОЛІТИКА СЕРТИФІКАТА ТА ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

4.1 Політика сертифіката

4.1.1 Перелік сфер, в яких дозволяється використання кваліфікованих сертифікатів відкритих ключів, сформованих Надавачем

Перелік сфер, в яких дозволяється використання кваліфікованих сертифікатів відкритих ключів, визначено в пункті 1.4.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

4.1.2 Обмеження щодо використання кваліфікованих сертифікатів відкритих ключів, сформованих Надавачем

Обмеження щодо використання кваліфікованих сертифікатів відкритих ключів визначено в пункті 1.4.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

4.1.3 Перелік інформації, що розміщується Надавачем на офіційному веб-сайті

В пункті 2.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) наведено перелік інформації, доступ до якої забезпечує Надавач через офіційний веб-сайт.

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

Час і порядок публікації кваліфікованих сертифікатів відкритих ключів та списків відкликаних сертифікатів визначено в пункті 2.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

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

Механізм підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа, визначено в пункті 3.2.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

4.1.6 Ідентифікація та автентифікація заявника під час формування кваліфікованого сертифіката відкритого ключа

Умови встановлення заявника (автентифікації особи) визначено в пункті 3.2.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) та пункті 3.2.2 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

Умови повноважень уповноваженого представника юридичної особи визначено в пункті 3.2.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) та пункті 3.2.4 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

4.1.7 Механізм автентифікації користувачів, які мають чинний кваліфікований сертифікат відкритого ключа

Механізм автентифікації користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, визначено в пункті 3.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) та пункті 3.3 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

4.1.8 Механізми автентифікації користувачів під час скасування, блокування або поновлення кваліфікованого сертифіката відкритого ключа

Механізм автентифікації користувачів під час скасування, блокування або поновлення кваліфікованого сертифіката відкритого ключа визначено в пункті 3.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) та пункті 3.4 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

4.1.9 Опис фізичного середовища

Місцезнаходження приміщень Надавача: 03142, м. Київ, вул. Ірпінська, 1 та 03134, м. Київ, вул. Пшенична, 4А.

Приміщення Надавача поділяються за функціональним призначенням на такі категорії:

- спеціальне приміщення, в якому встановлені технічні засоби та обладнання ПТК Надавача;
- адміністративні приміщення, в яких розміщуються робочі станції персоналу Надавача;
- архівні приміщення, в яких зберігаються документи на паперових носіях.

Фізичний доступ до приміщень, в яких розміщуються технічні засоби ПТК Надавача, обмежений і надається тільки співробітникам Надавача відповідно до їх службових обов'язків. Доступ сторонніх осіб до приміщень можливий лише в супроводі співробітників Надавача, яким надано такий доступ.

Процедура доступу до спеціальних приміщень Надавача визначена в пункті 5.1.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

4.1.10 Процедурний контроль

Положення щодо процедурного контролю визначені в пункті 5.2 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

4.1.11 Порядок ведення журналів аудиту подій

Типи подій, частота перегляду, строки зберігання журналів аудиту подій, методи захисту та резервного копіювання журналів аудиту подій, персонал Надавача, що може здійснювати перегляд журналів аудиту подій визначено в пункті 5.4 Політика сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

4.1.12 Порядок ведення архівів Надавача

Види документів та даних, що підлягають архівуванню, строки зберігання архівів, механізм та порядок зберігання і захисту архівів, періодичність створення резервних копій та правила збереження з'ємних носіїв визначені в пункті 5.5 Політики сертифікатів кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Архівні копії журналів аудиту подій мають зберігатися не менше 10 років. Контроль за здійсненням автоматичного резервного копіювання та виконання резервного копіювання в ручному режимі покладається на системного адміністратора. Адміністратор безпеки періодично контролює процес створення та зберігання резервних копій.

4.1.13 Процес, порядок та умови генерації пар ключів Надавача та користувачів

В ІКС Надавача використовуються особисті та відповідні їм відкриті ключі за такими призначеннями (сферою використання) та з такими параметрами:

- особисті та відповідні їм відкриті ключі Надавача для накладення та перевірки електронного підпису на кваліфікованих сертифікатах відкритих ключів підписувачів та СВС зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння", затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі - ДСТУ 4145-2002);
- особисті та відповідні їм відкриті ключі Надавача, що використовуються для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;
- особисті та відповідні їм відкриті ключі Надавача для накладення та перевірки електронного підпису на даних про статус кваліфікованих сертифікатів відкритих ключів підписувачів, що визначається в режимі реального часу, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;
- особисті та відповідні їм відкриті ключі серверів обробки запитів, що використовуються для криптографічного захисту повідомлень, які передаються

відкритими каналами зв’язку, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;

- особисті та відповідні їм відкриті ключі посадових осіб (адміністраторів), що використовуються для автентифікації посадових осіб та криптографічного захисту повідомлень, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002;
- особисті та відповідні їм відкриті ключі Надавача для накладення та перевірки електронного підпису на кваліфікованих сертифікатах відкритих ключів підписувачів та СВС із використанням іменованої еліптичної кривої NIST P-256 (secp256r1) для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2015 "Електронні підписи й інфраструктури (ESI). Криптографічні комплекти" (далі - ДСТУ ETSI EN 119 312:2015);
- особисті та відповідні їм відкриті ключі Надавача, що використовуються для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу із використанням іменованої еліптичної кривої NIST P-256 (secp256r1) для алгоритму ECDSA згідно з ДСТУ ETSI TS 119 312:2015;
- особисті та відповідні їм відкриті ключі Надавача для накладення та перевірки електронного підпису на даних про статус кваліфікованих сертифікатів відкритих ключів підписувачів, що визначається в режимі реального часу, із використанням іменованої еліптичної кривої NIST P-256 (secp256r1) для алгоритму ECDSA згідно з ДСТУ ETSI EN 119 312:2015;
- особисті та відповідні їм відкриті ключі Надавача для накладення та перевірки електронного підпису на кваліфікованих сертифікатах відкритих ключів підписувачів та СВС з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015;
- особисті та відповідні їм відкриті ключі Надавача, що використовуються для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу, з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015;
- особисті та відповідні їм відкриті ключі Надавача для накладення та перевірки електронного підпису на даних про статус кваліфікованих сертифікатів відкритих ключів підписувачів, що визначається в режимі реального часу, з довжиною ключа не менше 4096 біт для алгоритму RSA відповідно до ДСТУ ETSI EN 119 312:2015.

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

- для особистих ключів Надавача для накладення електронного підпису на кваліфіковані сертифікати відкритих ключів підписувачів та СВС - не більше 5 років;
- для особистих ключів Надавача, що використовуються для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу - не більше 5 років;
- для особистих ключів Надавача, що використовуються для накладення електронного підпису на даних про статус кваліфікованих сертифікатів відкритих ключів підписувачів, що визначається в режимі реального часу - не більше 2 років;

- для особистих ключів серверів обробки запитів, що використовуються для криптографічного захисту повідомлень - не більше 2 років;
- для особистих ключів посадових осіб - не більше 2 років.

Особисті ключі Надавача для накладення та перевірки електронного підпису на кваліфікованих сертифікатах відкритих ключів підписувачів та СВС, особисті ключі Надавача, що використовуються для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу та ключі Надавача для накладення та перевірки електронного підпису на даних про статус кваліфікованих сертифікатів відкритих ключів підписувачів, що визначається в режимі реального часу, генеруються, зберігаються та застосовуються виключно у засобах кваліфікованого електронного підпису чи печатки, що є апаратно-програмними пристроями і входять до складу ІКС Надавача.

4.1.13.1 Генерація особистих ключів Надавача та сервера TSP

Процедура генерації та резервного копіювання особистого ключа Надавача визначена в пункті 6.1.1.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Процедура резервного копіювання особистого ключа Надавача викладена в п.6.2.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Генерація особистих та відповідних їм відкритих ключів Надавача та сервера позначки часу (TSP) здійснюється у спеціальному приміщенні ІКС адміністратором сертифікації під контролем адміністратора безпеки.

Після генерації особистих та відкритих ключів запит на формування сертифіката Надавача або сервера TSP, що містить відповідний відкритий ключ, записується на з'ємний носій для подальшої передачі до ЦЗО.

4.1.13.2 Генерація особистих ключів серверів OCSP та серверів обробки запитів ІКС Надавача

Процедура генерації особистих ключів серверів OCSP та серверів обробки запитів ІКС Надавача є аналогічною до процедури генерації особистих ключів Надавача і визначена в пункті 6.1.1.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Процедура резервного копіювання особистих ключів серверів OCSP та серверів обробки запитів ІКС Надавача є аналогічною до процедури резервного копіювання особистих ключів Надавача і викладена в п.6.2.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Генерація особистих та відповідних їм відкритих ключів серверів OCSP та серверів обробки запитів ІКС Надавача здійснюється у спеціальному приміщенні ІКС адміністратором сертифікації під контролем адміністратора безпеки.

Після генерації особистих та відкритих ключів здійснюється формування відповідних сертифікатів ключів.

4.1.13.3 Генерація особистих ключів адміністраторів

Генерація особистих та відповідних їм відкритих ключів адміністраторів здійснюється особисто адміністраторами на власних робочих станціях у приміщеннях Надавача.

В процесі генерації особистий ключ адміністратора зберігається на ЗКЕП. Запит на формування сертифіката адміністратора, що містить відкритий ключ, записується на з'ємний диск для подальшої передачі адміністратору сертифікації.

Генерація особистого ключа адміністратора реєстрації ВПР може здійснюватися на робочій станції адміністратора реєстрації безпосередньо у приміщеннях відокремленого пункту реєстрації. В цьому випадку генерація ключів здійснюється адміністратором реєстрації самостійно, а запит на формування сертифіката адміністратора реєстрації передається до центрального офісу Надавача адміністратору сертифікації засобами електронної пошти чи на зовнішньому носії інформації.

4.1.13.4 Формування кваліфікованих сертифікатів відкритих ключів Надавача

Після генерації особистого ключа Надавача здійснюється формування запиту на кваліфікований сертифікат відкритого ключа Надавача у форматі PKCS#10. Формування запиту на кваліфікований сертифікат відкритого ключа Надавача виконується у службовому приміщенні Надавача з використанням особистого ключа Надавача за участю двох осіб – адміністратора безпеки та адміністратора сертифікації.

Після формування запиту на кваліфікований сертифікат відкритого ключа Надавача він передається до центрального засвідчувального органу відповідно до Регламенту роботи центрального засвідчувального органу, затвердженого наказом Міністерства цифрової трансформації України від 28 лютого 2024 р. № 33, зареєстрованого в Міністерстві юстиції України 15 березня 2024 р. за № 393/41738.

Після отримання кваліфікованого сертифіката відкритого ключа Надавача від центрального засвідчувального органу такий сертифікат записується у базу даних ПТК Надавача і публікується на офіційному веб-сайті Надавача.

4.1.13.5 Формування кваліфікованих сертифікатів відкритих ключів серверів ІКС Надавача (TSP, OCSP, серверів обробки запитів)

Після генерації особистого ключа сервера позначки часу (TSP) Надавача здійснюється формування запиту на кваліфікований сертифікат відкритого ключа сервера позначки часу (TSP) Надавача у форматі PKCS#10. Формування запиту виконується у службовому приміщенні Надавача з використанням особистого ключа сервера позначки часу (TSP) Надавача за участю двох осіб – адміністратора безпеки та адміністратора сертифікації.

Після формування запиту на кваліфікований сертифікат відкритого ключа сервера позначки часу (TSP) Надавача він передається до центрального засвідчувального органу відповідно до Регламенту роботи центрального засвідчувального органу, затвердженого наказом Міністерства цифрової трансформації України від 28 лютого 2024 р. № 33, зареєстрованого в Міністерстві юстиції України 15 березня 2024 р. за № 393/41738.

Після формування центральним засвідчувальним органом та отримання Надавачем кваліфікованого сертифіката відкритого ключа сервера позначки часу (TSP) Надавача такий сертифікат записується у базу даних ПТК Надавача і публікується на офіційному веб-сайті Надавача.

Формування кваліфікованих сертифікатів відкритих ключів серверів OCSP та серверів обробки запитів ІКС Надавача здійснюється адміністратором сертифікації з використанням чинного особистого ключа Надавача.

Після формування Надавачем кваліфікованих сертифікатів відкритих ключів серверів ІКС Надавача (OCSP та серверів обробки запитів) такі сертифікати публікуються на офіційному веб-сайті Надавача.

4.1.13.6 Формування кваліфікованих сертифікатів відкритих ключів адміністраторів

Після генерації особистих та відкритих ключів здійснюється формування відповідних сертифікатів ключів посадових осіб (адміністраторів).

Формування кваліфікованих сертифікатів відкритих ключів посадових осіб здійснюється адміністратором сертифікації з використанням чинного особистого ключа Надавача.

4.1.13.7 Планова заміна ключів Надавача

Процедура планової зміни ключів Надавача визначена в пункті 5.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

4.1.13.8 Планова заміна ключів серверів ІКС Надавача (TSP, OCSP, серверів обробки запитів)

Процедура планової зміни ключів серверів ІКС Надавача (OCSP, TSP, серверів обробки запитів) визначена в пункті 5.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Після початку використання нових особистих ключів серверів ІКС Надавача (OCSP, TSP, серверів обробки запитів) попередні особисті ключі та їх резервні копії знищуються способом, що унеможливлює їх відновлення, за участю адміністратора сертифікації та адміністратора безпеки.

Попередні відкриті ключі серверів ІКС Надавача (OCSP, TSP, серверів обробки запитів) зберігаються у складі відповідних кваліфікованих сертифікатів відкритих ключів постійно і використовуються для перевірки КЕП на раніше сформованих повідомленнях (позначках часу, інформації про статус сертифікатів тощо).

4.1.13.9 Планова заміна ключів адміністраторів

Планова зміна особистих ключів адміністраторів виконується до завершення термінів дії закінчення строку дії відповідних сертифікатів відкритих ключів.

Під час планової заміни ключів адміністратор відповідно до вимог п. 4.1.13.3 Регламенту здійснює генерацію нових особистого та відповідного йому відкритого ключа.

Після початку використання нових особистих ключів адміністраторів попередні кваліфіковані сертифікати відкритих ключів адміністраторів скасовуються адміністратором сертифікації, попередні особисті ключі знищуються способом, що унеможливлює їх відновлення.

Попередні відкриті ключі адміністраторів зберігаються у складі відповідних кваліфікованих сертифікатів відкритих ключів постійно.

4.1.13.10 Позапланова заміна ключів Надавача, серверів ІКС Надавача та адміністраторів

Процедура позапланової зміни ключів відповідає процедурі, визначеній в пункті 5.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Порядок дій персоналу Надавача у разі компрометації або підозри на компрометацію особистих ключів визначено в пункті 5.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Після офіційного оповіщення підписувачів та створювачів електронних печаток про факт позапланової зміни ключів Надавач забезпечує виконання процедур одержання підписувачами та створювачами електронних печаток нових кваліфікованих сертифікатів відкритих ключів відповідно до вимог цього Регламенту.

Позапланова заміна особистих та відповідних їм відкритих ключів Надавача, серверів ІКС Надавача або посадових осіб Надавача здійснюється у випадках компрометації або підозри на компрометацію особистих ключів.

Під час позапланової заміни ключів Надавача адміністратором сертифікації і адміністратором безпеки здійснюється генерація нових особистого та відповідного йому відкритого ключа відповідно до вимог п. 4.1.13.1 Регламенту.

Надавач негайно інформує ЦЗО про факт компрометації особистого ключа Надавача з метою скасування відповідного сертифіката.

Всі сертифікати відкритих ключів підписувачів Надавача, серверів ІКС Надавача та посадових осіб Надавача, що були сформовані з використанням скомпрометованого особистого ключа, скасовуються. Список відкликаних сертифікатів підписується новим особистим ключем Надавача.

Сертифікати відкритих ключів, що були скасовані через компрометацію ключа Надавача, повинні бути позапланово сформовані повторно з використанням нового особистого ключа Надавача.

Під час позапланової заміни ключів серверів ІКС Надавача адміністратором сертифікації і адміністратором безпеки здійснюється генерація нових особистого та відповідного йому відкритого ключа відповідно до вимог п. 4.1.13.1 або 4.1.13.2 Регламенту.

Попередні сертифікати відкритих ключів серверів ІКС Надавача, що відповідають скомпрометованим ключам, скасовуються Надавачем (крім випадку компрометації особистого ключа сервера TSP). У разі компрометації особистого ключа сервера TSP Надавач негайно інформує ЦЗО про факт компрометації особистого ключа з метою скасування відповідного сертифіката.

Під час позапланової заміни ключів посадової особи здійснюється генерація нових особистого та відповідного йому відкритого ключа посадовою особою відповідно до вимог п. 4.1.13.3 Регламенту. Попередні сертифікати відкритих ключів посадових осіб, що відповідають скомпрометованим ключам, скасовуються Надавачем.

Усі особисті ключі, факт компрометації яких було підтверджено, знищуються способом, що унеможливлює їх відновлення.

4.1.13.11 Генерація ключів користувачів

Процедура генерації ключів користувачів визначена в пункті 6.1.1.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

4.1.13.12 Процедура ідентифікації користувачем відокремлених пунктів реєстрації Надавача

Ідентифікація користувачем відокремленого пункту реєстрації Надавача здійснюється шляхом перевірки на офіційному веб-сайті Надавача інформації про адресу розташування, графік роботи та контакти такого відокремленого пункту реєстрації.

4.1.14 Процедура отримання користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги її Надавачем

Процедура отримання користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги визначена в пункті 6.1.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

4.1.15 Механізм надання відкритого ключа користувача Надавачу для формування кваліфікованого сертифіката відкритого ключа

Механізм надання відкритого ключа користувача Надавачу для формування кваліфікованого сертифіката відкритого ключа визначено у пункті 6.1.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

4.1.16 Порядок захисту та доступу до особистого ключа Надавача та серверів ІКС Надавача

4.1.16.1 Порядок зберігання ключових даних

Особисті ключі Надавача та серверів ІКС Надавача зберігаються в апаратно-програмних засобах КЕП і можуть бути експортовані з них на інші апаратно-програмні засоби КЕП виключно з метою створення резервної копії.

4.1.16.2 Порядок зберігання носіїв ключової інформації

Апаратно-програмні засоби КЕП з резервними копіями особистого ключа Надавача та особистих ключів серверів ІКС Надавача зберігаються у спеціальному приміщенні в запечатаних конвертах чи коробках, які засвідчуються підписом адміністратора безпеки та печаткою Надавача.

4.1.16.3 Заходи безпеки під час генерації ключових даних

Генерація ключових даних (особистих та відкритих ключів) здійснюється згідно з експлуатаційною документацією на відповідні технічні засоби ІКС Надавача, на яких здійснюється генерація.

Генерація особистих ключів Надавача та особистих ключів серверів ІКС Надавача здійснюється у спеціальному приміщенні Надавача.

Під час генерації особистих ключів Надавача та особистих ключів серверів ІКС Надавача двері до спеціального приміщення повинні бути зачиненими, а всі дії проводитись або всередині приміщення, або за допомогою віддаленого робочого столу на робочій станції адміністратора безпеки.

4.1.16.4 Порядок знищення особистих ключів Надавача та серверів ІКС Надавача

Порядок знищення особистих ключів Надавача та серверів ІКС Надавача визначено в пункті 6.2.10 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

4.1.17 Порядок та умови резервного копіювання особистого ключа Надавача, серверів ІКС Надавача, адміністраторів, збереження, доступу та використання резервних копій

Для забезпечення можливості відновлення особистих ключів Надавача та серверів ІКС Надавача у разі виходу з ладу засобів кваліфікованого електронного підпису чи печатки, що є апаратно-програмними пристроями, виконується резервне копіювання відповідних особистих ключів із такого засобу виключно на засоби кваліфікованого електронного підпису чи печатки.

Порядок та умови резервного копіювання особистого ключа Надавача, серверів ІКС Надавача визначено в пункті 6.2.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Резервна копія записується на зовнішній засіб КЕП, який є апаратно-програмним пристроєм, у захищеному вигляді, що забезпечує цілісність та конфіденційність ключів.

Резервні копії особистих ключів Надавача та серверів ІКС Надавача можуть бути застосовані у випадку виходу з ладу засобів кваліфікованого електронного підпису чи печатки, в яких зберігалися та використовувалися відповідні особисті ключі, для відновлення ключів у відремонтованому або заміненому засобі кваліфікованого електронного підпису чи печатки.

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

Умови забезпечення захисту резервних копій особистих ключів Надавача та серверів ІКС Надавача під час їх зберігання повинні бути не гіршими, ніж умови забезпечення захисту особистих ключів, що використовуються в ІКС.

Резервне копіювання особистих ключів посадових осіб (адміністраторів) не виконується.

4.2 Положення сертифікаційних практик

4.2.1 Процес подання запиту на формування кваліфікованого сертифіката відкритого ключа

Порядок подання запиту на формування кваліфікованого сертифіката відкритого ключа визначено в пункті 4.1 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

4.2.2 Порядок надання сформованого кваліфікованого сертифіката відкритого ключа користувачу

Порядок надання сформованого кваліфікованого сертифіката відкритого ключа користувачу визначено в пункті 4.3 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

Послідовність дій користувача щодо перевірки даних, що містяться в сформованому кваліфікованому сертифікаті відкритого ключа, визначено в пункті 4.4 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

4.2.3 Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа користувача на офіційному веб-сайті Надавача

Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа користувача на офіційному веб-сайті Надавача визначено в пункті 2.2.1 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

4.2.4 Умови використання кваліфікованого сертифіката відкритого ключа користувача та його особистого ключа

Умови використання електронних довірчих послуг користувачами визначено в пункті 1.3.3.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Кваліфіковані сертифікати відкритого ключа підписувачів та створювачів електронної печатки використовуються у сферах та із обмеженнями, зазначеними у пунктах 1.4.1 та 1.4.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Наслідками неправильного використання кваліфікованого сертифіката відкритого ключа та особистого ключа можуть стати недостовірна автентифікація підписувача або створювача електронної печатки в інформаційних системах, заволодіння зловмисниками правами доступу користувача до інформації, підробка електронних документів, матеріальні та репутаційні втрати користувача.

4.2.5 Процедура подачі запиту на формування кваліфікованого сертифіката відкритого ключа для користувачів, які мають чинний кваліфікований сертифікат відкритого ключа

Порядок подачі запиту на формування кваліфікованого сертифіката відкритого ключа для користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, визначено в пункті 4.7 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

4.2.6 Обставини зміни статусу (скасування, блокування, поновлення) кваліфікованого сертифіката відкритого ключа

Перелік обставин для зміни статусу кваліфікованого сертифіката відкритого ключа визначено в пункті 3.4 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

Порядок блокування та скасування кваліфікованого сертифіката відкритого ключа визначено в пункті 4.9 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

Порядок формування списків відкликаних сертифікатів, публікація та розповсюдження списків відкликаних сертифікатів визначено в пункті 2.3 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту).

4.2.7 Строк закінчення дії кваліфікованого сертифіката відкритого ключа користувача

Строк дії кваліфікованих сертифікатів відкритих ключів користувачів становить не більше двох років.

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

Після закінчення строку дії кваліфікованого сертифіката такий кваліфікований сертифікат відкритого ключа вважається нечинним.

5.ПРОЦЕДУРИ ТА ПРОЦЕСИ, ЯКІ ВИКОНУЮТЬСЯ ПІД ЧАС НАДАННЯ КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, ЩО НЕ ПЕРЕДБАЧАЮТЬ ФОРМУВАННЯ ТА ОБСЛУГОВУВАННЯ КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ

5.1 Надання засобів кваліфікованого електронного підпису чи печатки

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

Надання Надавачем засобів кваліфікованого електронного підпису чи печатки у вигляді апаратно-програмних засобів та їх технічна підтримка і обслуговування здійснюється на договірних засадах.

Надання Надавачем засобів кваліфікованого електронного підпису чи печатки у вигляді окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків, може здійснюватись шляхом передачі цих засобів на носіях інформації безпосередньо підписувачу або створювачу електронної печатки або шляхом надання доступу через офіційний веб-сайт Надавача.

Надавачем на договірних засадах може здійснюватися надання доступу до частини ресурсу засобу кваліфікованого електронного підпису, який реалізує зберігання множини особистих ключів кваліфікованого електронного підпису чи печатки (наприклад, мережний криптомодуль).

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

Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження кваліфікованої електронної позначки часу надається користувачам в режимі реального часу за протоколом TSP.

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

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

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

Додаток 1
до Регламенту роботи кваліфікованого
надавача електронних довірчих послуг
ТОВ «Центр сертифікації ключів «Україна»

ПОЛІТИКА СЕРТИФІКАТА
КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ
ТОВ «ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ «УКРАЇНА»

Зміст

3.1. Позначення

3.1.1. Типи позначень сертифіката

3.1.2. Позначення (реквізити та атрибути) сертифікатів

3.1.3. Анонімність або використання псевдонімів

3.1.4. Правила інтерпретації різних форм позначень сертифіката

3.1.5. Унікальність позначень сертифіката

3.1.6. Визнання, автентифікація та роль торгових марок

3.2. Первинна перевірка ідентифікації

3.2.1. Метод підтвердження володіння особистим ключем

3.2.2. Автентифікація особи

3.2.3. Неперевірена інформація про користувача

3.2.4. Підтвердження повноважень

3.3. Ідентифікація та автентифікація при повторному формуванні кваліфікованих сертифікатів відкритого ключа

3.3.1. Ідентифікація та автентифікація користувача при повторному формуванні сертифіката за умови чинності попереднього сертифіката

3.3.2. Ідентифікація та автентифікація користувача при повторному формуванні кваліфікованих сертифікатів відкритого ключа у разі скасування сертифіката

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

4. Вимоги до життєвого циклу сертифіката

4.1. Заява на формування сертифіката

4.2. Обробка запиту на формування сертифіката

4.3. Формування сертифіката

4.4. Прийняття сертифіката

4.5. Використання пари ключів і сертифіката

4.5.1. Використання особистого ключа та сертифіката користувачем

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

4.6. Поновлення сертифіката

4.7. Повторне формування сертифіката

4.8. Зміна сертифіката

4.9. Скасування та блокування сертифіката

4.10. Служби статусу сертифіката

4.11. Закінчення строку дії сертифіката

4.12. Депонування та повернення ключів

5. Об’єкт, управління та операційний контроль

5.1. Контроль фізичної безпеки

5.1.1. Вимоги до приміщень Надавача

5.1.2. Фізичний доступ

5.2. Процедурний контроль

5.3. Контроль персоналу

5.3.1. Довірені ролі персоналу

5.3.1.1. Керівник

5.3.1.2. Адміністратор реєстрації

5.3.1.3. Адміністратор сертифікації

5.3.1.4. Адміністратор безпеки

5.3.1.5. Системний адміністратор

5.3.1.6. Аудитор системи

5.3.2. Вимоги щодо кваліфікації, досвіду та допуску персоналу

5.3.3. Вимоги та процедури навчання персоналу

5.3.4. Санкції за несанкціоновані дії персоналу

5.3.5. Контроль відокремлених пунктів реєстрації

5.3.6. Документація, яка надається персоналу

5.4. Ведення журналу аудиту подій

5.4.1. Типи записаних подій

5.4.2. Частота обробки журналу аудиту подій

5.4.3. Строки зберігання журналу аудиту подій

5.4.4. Захист журналу аудиту подій

5.4.5. Процедури резервного копіювання журналу аудиту подій

5.4.6. Синхронізація часу

5.5. Архів документів

5.5.1. Види документів та даних, що підлягають архівному зберіганню

5.5.2. Строки зберігання архіву

5.5.3. Захист архіву

5.5.4. Процедури резервного копіювання архіву

5.5.5. Вимога щодо накладання електронних позначок часу на записи

5.5.6. Система збирання архівів (внутрішня чи зовнішня)

5.5.7. Процедури отримання та перевірки архівної інформації

5.6. Зміна ключа

5.7. Компрометація і аварійне відновлення

5.7.1. Процедури обробки інцидентів і компрометації

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

5.7.3. Процедури відновлення після компрометації ключа

5.7.4. Можливості безперервності бізнесу після катастрофи

5.8. Припинення діяльності Надавача

5.8.1. Підстави припинення діяльності Надавача

5.8.2. Повідомлення про припинення діяльності Надавача

5.8.3. Дата припинення діяльності Надавача

5.8.4. Правонаступництво

5.8.5. Передача документованої інформації

5.8.6. План припинення діяльності

6. Технічні заходи безпеки

6.1. Генерація та встановлення пари ключів

6.1.1. Генерація пари ключів

6.1.1.1. Генерація пари ключів Надавача

6.1.1.2. Генерація пари ключів користувача

6.1.2. Доставка особистого ключа користувачу

6.1.3. Доставка відкритого ключа користувачу

6.1.4. Доставка відкритого ключа Надавача суб'єктам, які довіряють Надавачу

6.1.5. Розміри (параметри) ключів

6.1.6. Генерація параметрів відкритого ключа

6.1.7. Основні цілі використання особистого ключа надавачем

6.2. Захист особистого ключа та інженерний контроль криптографічного модуля

6.2.1. Стандарти та елементи керування криптографічним модулем

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

6.2.3. Управління особистим ключем підписувача

6.2.4. Резервне копіювання особистого ключа

6.2.5. Архівація особистого ключа

6.2.6. Відновлення особистого ключа

6.2.7. Зберігання особистого ключа в криптографічному модулі

6.2.8. Активація особистих ключів

6.2.9. Деактивація особистих ключів

6.2.10. Знищення особистих ключів

6.2.11. Можливості мережного криптографічного модуля

6.3. Інші аспекти керування парами ключів

6.3.1. Архівація відкритого ключа

6.3.2. Строки дії сертифіката та строки використання пари ключів

6.4. Дані активації

6.4.1. Створення та встановлення даних активації

6.4.2. Захист даних активації

6.4.3. Інші аспекти даних активації

6.5. Контроль комп'ютерної безпеки

6.5.1. Спеціальні технічні вимоги до комп’ютерної безпеки

6.5.2. Рейтинг комп’ютерної безпеки

6.6. Контроль безпеки життєвого циклу

6.6.1. Контроль розробки системи

6.6.2. Засоби керування безпекою

6.6.3. Контроль безпеки протягом життєвого циклу

6.7. Контроль безпеки мережі

6.8. Електронні позначки часу

6.8.1. Формування кваліфікованої електронної позначки часу

6.8.2. Перевірка кваліфікованої електронної позначки часу

6.8.3. Недійсність кваліфікованої електронної позначки часу

6.8.4. Отримання кваліфікованої електронної позначки часу Надавачем

7. Профілі сертифікатів, списків відкликаних сертифікатів та протоколу визначення статусу сертифіката

7.1. Профілі сертифікатів

7.2. Профілі списку відкликаних сертифікатів

7.3. Профілі протоколу визначення статусу сертифіката

8. Аудит відповідності та інші оцінки

8.1. Частота або обставини оцінювання

8.2. Особа/кваліфікація оцінювача

8.2.1. Вимоги до кваліфікації контролюючого органу (КО)

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

8.3. Відносини експерта з об’єктом оцінки

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

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

8.4. Теми, охоплені оцінюванням

8.4.1. Питання, що підлягають перевірці під час державного контролю

8.4.2. Питання, що підлягають перевірці під час оцінки відповідності

8.5. Дії, вжиті внаслідок порушення

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

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

8.6. Повідомлення результатів

8.6.1. Оформлення результатів державного контролю

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

8.6.3. Оформлення результатів оцінки відповідності

8.7. Самоперевірки

9. Інші комерційні та юридичні питання

9.1. Збори

9.1.1. Плата за видачу або поновлення сертифіката

9.1.2. Плата за доступ до сертифіката

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

9.1.4. Плата за інші послуги

9.1.5. Політика відшкодування

9.2. Фінансова відповідальність

9.3. Конфіденційність ділових даних

9.3.1. Обсяг конфіденційної інформації

9.3.2. Інформація, що не належить до конфіденційної

9.3.3. Відповідальність за захист конфіденційної інформації

9.4. Захист персональних даних

9.4.1. Концепція захисту персональних даних

9.4.2. Визначення персональних даних

9.4.3. Персональні дані, що не вважаються конфіденційними

9.4.4. Відповідальність за захист персональних даних

9.4.5. Інформація та згода на використання персональних даних

9.4.6. Розкриття персональних даних

9.5. Права інтелектуальної власності

9.6. Заяви та гарантії

9.6.1. Зобов’язання та гарантії Надавача

9.6.2. Зобов’язання та гарантії відокремлених пунктів реєстрації

9.6.3. Зобов’язання та гарантії користувачів

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

9.6.5. Зобов’язання та гарантії інших учасників

9.7. Відмова від відповідальності

9.8. Обмеження відповідальності

9.9. Відшкодування збитків

9.10. Термін дії та припинення дії

9.11. Індивідуальні повідомлення та комунікації з учасниками інфраструктури відкритих ключів

9.12. Зміни

9.13. Положення щодо вирішення спорів

9.14. Застосовне право

9.15. Дотримання чинного законодавства

1. ВСТУП

1.1. Огляд

Ця Політика сертифіката визначає перелік усіх правил, що застосовуються кваліфікованим надавачем електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (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 Надавача та найманих працівників Надавача, посадові обов'язки яких безпосередньо пов'язані з реєстрацією користувачів, формуванням та обслуговуванням кваліфікованих сертифікатів (далі - персонал), а також фізичних та юридичних осіб, які на підставі договорів, укладених з Надавачем (ТОВ «Центр сертифікації ключів «Україна») безпосередньо чи опосередковано пов'язані з реєстрацією користувачів, формуванням та/або обслуговуванням кваліфікованих сертифікатів, 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 Надавача.

Ця Політика сертифіката відповідає вимогам, визначеним у:

- ДСТУ ETSI EN 319 411-1 (ETSI EN 319 411-1) «Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги» (далі - ДСТУ ETSI EN 319 411-1);
- ДСТУ ETSI EN 319 411-2 (ETSI EN 319 411-2) «Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС» (далі - ДСТУ ETSI EN 319 411-2);
- ДСТУ ETSI EN 319 412-2 (ETSI EN 319 412-2, IDT) «Електронні підписи та інфраструктури. (ESI). Профілі сертифікатів. Частина 2. Профілі сертифікатів, виданих фізичним особам» (далі - ДСТУ ETSI EN 319 412-2);
- ДСТУ ETSI EN 319 401 (ETSI EN 319 401, IDT) «Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг» (далі - ДСТУ ETSI EN 319 401).

1.2. Назва документа та його ідентифікація

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

Повна назва документа: Політика сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна».

Скорочена назва документа: Політика сертифіката КНЕДП ТОВ «Центр сертифікації ключів «Україна».

Версія: 1.0.

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

Об'єктний ідентифікатор (OID) цієї Політики сертифіката присвоєно відповідно до стандарту ASN.1 згідно з вмістом наведеної нижче таблиці.

Таблиця 1. Структура об'єктного ідентифікатора (OID) Політики сертифіката

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

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

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 та ДСТУ ETSI EN 319 411-2.

1.3.1. Надавач

Надавач 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, формування та обслуговування їхніх кваліфікованих сертифікатів, в тому числі, управління їхнім статусом (блокування, поновлення та скасування).

Надавач здійснює реєстрацію користувачів самостійно та/або через відокремлені пункти реєстрації.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

1.3.1.1. Права Надавача

Надавач має право:

- надавати електронні довірчі послуги з дотриманням вимог законодавства у сфері електронних довірчих послуг;
- отримувати документи та/або електронні дані, необхідні для ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті;
- проводити під час формування та видачі кваліфікованих сертифікатів перевірку інформації про осіб, яким видаються такі сертифікати, з використанням відомостей інформаційних ресурсів ЄІС МВС (відомостей, що містяться в ЄДДР, та відомостей щодо викрадених (втрачених) документів за зверненнями громадян), ДРФО, ДРАЦС, ЄДР, а також інформації з інших публічних електронних реєстрів відповідно до Закону України "Про публічні електронні реєстри", отриманих у процесі електронної взаємодії за допомогою інтегрованої системи електронної ідентифікації (https://id.gov.ua/);
- отримувати консультації від ЦЗО, КО з питань, пов'язаних з наданням електронних довірчих послуг;
- звертатися до ООВ для отримання документів про відповідність;
- звертатися до ЦЗО із заявами про формування кваліфікованих сертифікатів, їх скасування, блокування або поновлення;
- самостійно обирати в рамках кожної послуги, які саме стандарти він буде застосовувати для надання кваліфікованих електронних довірчих послуг, з переліку стандартів, визначеного Кабінетом Міністрів України.

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 ІКС 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-сайті відомостей з реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

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

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

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

– скасування, блокування та поновлення кваліфікованих сертифікатів відповідно до вимог Закону України "Про електронну ідентифікацію та електронні довірчі послуги";

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

– внесення даних користувача до відповідного кваліфікованого сертифіката;

– вжиття організаційних і технічних заходів з управління ризиками, пов'язаними з безпекою електронних довірчих послуг;

– інформування КО 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, без необґрунтованої затримки, не пізніше ніж протягом 24 годин з моменту, коли їм 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 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 кваліфікованих сертифікатів;

– постійне зберігання документів та електронних даних, отриманих у зв'язку з наданням електронних довірчих послуг;

– внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) для забезпечення відшкодування шкоди, яка може бути завдана користувачам чи третім особам внаслідок неналежного виконання Надавачем своїх зобов'язань, або страхування цивільно-правової відповідальності для забезпечення відшкодування такої шкоди у розмірі, визначеному Законом України "Про електронну ідентифікацію та електронні довірчі послуги";

– відновлення розміру внеску на поточному рахунку із спеціальним режимом використання у банку (на рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або розміру страхової суми, визначеного Законом України "Про електронну ідентифікацію та електронні довірчі послуги", протягом трьох місяців у разі зміни розміру мінімальної заробітної плати або в разі відшкодування збитків, завданих користувачам чи третім особам внаслідок неналежного виконання своїх зобов'язань;

- використання під час надання кваліфікованих електронних довірчих послуг виключно кваліфікованих сертифікатів, сформованих ЦЗО;
- 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 КО та ЦЗО про намір припинити свою діяльність та про зміни у наданні кваліфікованих електронних довірчих послуг протягом 48 годин з моменту настання таких змін;
- передачу ЦЗО або іншому надавачу документованої інформації в разі припинення діяльності з надання кваліфікованих електронних довірчих послуг;
- приєднання до програмного інтерфейсу ІКС ЦЗО з метою забезпечення інтероперабельності, дослідження поточного стану, перспектив розвитку сфери електронних довірчих послуг та виконання інших повноважень.

1.3.2. Органи реєстрації

Відокремлені пункти реєстрації Надавача є органами реєстрації, що представлені окремими підрозділами Надавача або юридичними чи фізичними особами, які на підставі договору з Надавачем здійснюють реєстрацію користувачів.

До працівників відокремлених пунктів реєстрації Надавача, на яких покладено обов'язки з реєстрації користувачів, застосовуються такі ж вимоги, як і до адміністраторів реєстрації, що визначені у пункті 5.3.1.2 цієї Політики сертифіката.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

1.3.3. Користувачі

Користувачами є підписувачі та створювачі електронних печаток, щодо яких Надавач здійснює їх реєстрацію (самостійно або через відокремлені пункти реєстрації Надавача), формування та обслуговування їхніх кваліфікованих сертифікатів.

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

- підписувач - фізична особа, яка створює електронний підпис;
- створювач електронної печатки - юридична особа або фізична особа - підприємець, яка створює електронну печатку.

1.3.3.1. Права користувачів

Користувачі мають право на:

- отримання електронних довірчих послуг;

– вільний вибір надавача;
– оскарження у судовому порядку дій чи бездіяльності надавача та органів, що здійснюють державне регулювання у сфері електронних довірчих послуг;
– відшкодування завданої їм шкоди та захист своїх прав і законних інтересів;
– звернення із заявою про скасування, блокування та поновлення свого кваліфікованого сертифіката.

1.3.3.2. Обов'язки користувачів

Користувачі зобов'язані:

– забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;
– невідкладно повідомляти надавача 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 про надання кваліфікованих електронних довірчих послуг, укладеним з надавачем;
– 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.

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:

– 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 та ДСТУ ETSI EN 319 411-2.

Крім того, застосовуються такі особливі вимоги:

1.4.1. Дозволене використання сертифіката

1.4.1.1. Види кваліфікованих сертифікатів

Надавач формує кваліфіковані сертифікати таких видів:

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

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

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

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

1.4.1.2. Строк дії кваліфікованих сертифікатів

Кваліфіковані сертифікати Надавача та сервера TSP Надавача формуються ЦЗО зі строком дії не більше 5 років.

Строки дії сертифікатів інших серверів ІКС Надавача та посадових осіб Надавача становлять не більше 2 років.

Кваліфіковані сертифікати користувачів формуються Надавачем зі строком дії не більше 2 років.

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

Відповідні Положення сертифікаційних практик Надавача містять додаткову інформацію.

1.4.2. Заборонене використання сертифіката

Кваліфікований сертифікат може використовуватися лише відповідно до зазначеного у ньому призначення відкритого ключа («keyUsage»).

1.4.3. Використання тестових сертифікатів

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

1.5. Управління Політикою сертифіката

1.5.1. Відповідальність за Політику сертифіката

Ця Політика сертифіката підтримується ТОВ «Центр сертифікації ключів «Україна».

ТОВ «Центр сертифікації ключів «Україна» є зареєстрованою відповідно до законодавства юридичною особою.

Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені ТОВ «Центр сертифікації ключів «Україна» або від імені відокремленого пункту реєстрації Надавача.

Реквізити ТОВ «Центр сертифікації ключів «Україна»:

- Код згідно з Єдиним державним реєстром підприємств та організацій України (ЄДРПОУ): 36865753.
- Адреса: Україна, 03142, м. Київ, вул. Ірпінська, 1.
- Контактний телефон: +38 (044) 206-72-30.

– Адреса електронної пошти: info@uakey.com.ua.

Реквізити Надавача:

– Адреса веб-сайту: uakey.com.ua.
– Контактний телефон: +38 (044) 206-72-31.
– Адреса електронної пошти: info@uakey.com.ua.

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

Ця Політика сертифіката, а також зміни до неї затверджуються директором ТОВ «Центр сертифікації ключів «Україна».

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

1.5.2. Внесення змін до Політики сертифіката

Відповідно до пункту 9.12 цієї Політики сертифіката.

1.6. Визначення термінів та перелік скорочень

1.6.1. Визначення термінів

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

1.6.2. Перелік скорочень

ВПР	Відокремлений пункт реєстрації
ДРАЦС	Державний реєстр актів цивільного стану громадян
ДРФО	Державний реєстр фізичних осіб - платників податків
ЄДДР	Єдиний державний демографічний реєстр
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань

ЄДРПОУ	Єдиний державний реєстр підприємств та організацій України
ЄІС МВС	Єдина інформаційна система Міністерства внутрішніх справ України
ЗКЕП	Засіб кваліфікованого електронного підпису чи печатки
ІКС	Інформаційно-комунікаційна система
КЕП	Кваліфікований електронний підпис
КЗІ	Криптографічний захист інформації
КНЕДП	Кваліфікований надавач електронних довірчих послуг
КО	Контролюючий орган (Адміністрація державної служби спеціального зв'язку та захисту інформації України)
КСЗІ	Комплексна система захисту інформації
ООВ	Орган з оцінки відповідності
ОС	Операційна система
ПЗ	Програмне забезпечення
ПТК	Програмно-технічний комплекс - апаратно-програмні та програмні засоби, що забезпечують виконання функцій КНЕДП
РНОКПП	Реєстраційний номер облікової картки платника податків
ЦЗО	Центральний засвідчувальний орган (Міністерство цифрової трансформації України)
OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol

2. ОБОВ'ЯЗКИ ЩОДО ПУБЛІКАЦІЇ ТА ЗБЕРІГАННЯ

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

Крім того, застосовуються такі особливі вимоги:

2.1. Репозиторій/вебсайт

Надавач повинен забезпечувати:

– 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.

Надавач через веб-сайт Надавача (https://uakey.com.ua) забезпечує вільний доступ до:

– відомостей про Надавача;

– даних про внесення відомостей про Надавача до Довірчого списку;

– Політики сертифіката Надавача;

– відповідних Положень сертифікаційних практик Надавача;

– загальних положень та умов надання кваліфікованих електронних довірчих послуг користувачам Надавача;

– кваліфікованих сертифікатів Надавача;

– переліку кваліфікованих електронних довірчих послуг, які надає Надавач;

– даних про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг Надавачем;

– форм документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;

– відомостей про відокремлені пункти реєстрації Надавача;

– реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;

– відомостей про обмеження під час використання кваліфікованих сертифікатів користувачами;

– даних про порядок перевірки чинності кваліфікованого сертифіката, у тому числі умови перевірки статусу сертифіката;

– переліку актів законодавства у сфері електронних довірчих послуг.

Ця Політика сертифіката доступна 24 години на добу 7 днів на тиждень у форматі лише для читання на веб-сайті Надавача.

Надавач забезпечує регулярне оновлення інформації та публікацію кваліфікованих сертифікатів, цієї Політики сертифіката, відповідних Положень сертифікаційних практик, списків відкликаних сертифікатів, договорів, актів законодавства та інших нормативних документів на веб-сайті Надавача.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

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 кваліфікованих електронних довірчих послуг.

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

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

2.2.2. Публікація сертифікатів Надавача

Кваліфіковані сертифікати Надавача повинні публікуватися на веб-сайті Надавача одразу після їх отримання від ЦЗО.

Кваліфіковані сертифікати серверів Надавача публікуються одразу після їх формування Надавачем.

Надавач забезпечує регулярне оновлення інформації та публікацію кваліфікованих сертифікатів, цієї Політики сертифіката, відповідних Положень сертифікаційних практик Надавача, списків відкликаних сертифікатів, договорів, законодавчих актів та інших нормативних документів на веб-сайті Надавача: https://uakey.com.ua.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

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.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

2.2.4. Строк закінчення дії сертифіката

Строки дії сертифікатів становлять:

- для сертифікатів Надавача для накладення електронного підпису на кваліфіковані сертифікати відкритих ключів підписувачів та СВС - не більше 5 років;
- для сертифікатів Надавача, що використовуються для надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу - не більше 5 років;
- для сертифікатів Надавача, що використовуються для накладення електронного підпису на даних про статус кваліфікованих сертифікатів відкритих ключів підписувачів, що визначається в режимі реального часу - не більше 2 років;

– для сертифікатів серверів обробки запитів, що використовуються для криптографічного захисту повідомлень - не більше 2 років;

– для сертифікатів посадових осіб - не більше 2 років.

Строк дії кваліфікованих сертифікатів користувачів становить не більше двох років.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

2.3. Час та періодичність публікації

Кваліфіковані сертифікати відкритих ключів Надавача публікуються одразу після їх отримання від Центрального засвідчувального органу.

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

Кваліфіковані сертифікати відкритих ключів підписувачів та створювачів електронної печатки, які надали згоду на їх публікацію, публікуються одразу після формування таких сертифікатів.

В подальшому режим публікації сертифіката може бути змінений за вимогою підписувача або створювача електронної печатки шляхом подання відповідної заяви в письмовому або електронному вигляді.

Надавач формує списки відкликаних сертифікатів у вигляді повного та часткового списків, які відповідають таким вимогам:

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

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

- на список відкликаних сертифікатів повинен бути накладений кваліфікований електронний підпис Надавача.

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

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

Посилання на списки відкликаних сертифікатів вносяться до кваліфікованих сертифікатів відкритих ключів підписувачів та створювачів електронної печатки.

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

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

У випадку одночасного використання Надавачем декількох діючих особистих ключів і відповідних до них сертифікатів Надавач може вести декілька списків відкликаних сертифікатів, підписаних різними особистими ключами. В такому разі всі вони публікуються на веб-сайті Надавача у наведеному вище порядку.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

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.

Захист інформації на веб-сайті, в репозиторії та базі даних Надавача здійснюється відповідно до вимог документації комплексної системи захисту інформації або системи управління інформаційною безпекою.

3. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

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

3.1. Позначення

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

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

Таблиця 2. Позначення, що використовуються в кваліфікованих сертифікатах користувачів

Найменування	Значення
Country (C)	Назва країни відповідно до ДСТУ ISO 3166-1:2009 «Коди назв країн світу» (ISO 3166-1:2006, IDT), затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 23 грудня 2009 р. № 471

Organization (O)	Найменування юридичної особи для кваліфікованого сертифіката юридичної особи або кваліфікованого сертифіката представника юридичної особи. Для кваліфікованих сертифікатів фізичних осіб, які не належать до юридичної особи, це поле недоступне
Organizational Unit (OU)	Назва підрозділу або відділу в організації. Для кваліфікованих сертифікатів фізичних осіб, які не належать до юридичної особи, це поле недоступне
State or Province (S)	Назва області місцезнаходження або місця реєстрації користувача
Locality (L)	Назва міста місцезнаходження або місця реєстрації користувача
Common Name (CN)	Повне ім'я (найменування) користувача, якому належить кваліфікований сертифікат
E-Mail Address (E)	Електронна пошта користувача, якому належить кваліфікований сертифікат
Title (T)	Посада (для кваліфікованих сертифікатів представників юридичної особи за необхідності)

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг «ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

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 позначення (реквізити, атрибути), визначені в стандартах щодо профілів сертифікатів відповідно до пункту 7.1, розділу 7 цієї Політики сертифіката.

3.1.3. Анонімність або використання псевдонімів

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» та ДСТУ ETSI EN 319 412-2.

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 гарантувати, що сертифікати з однаковими даними, зазначеними в полях «Common Name» та «SerialNumber», не видаються різним користувачам.

3.1.6. Визнання, автентифікація та роль торгових марок

Не застосовується.

3.2. Первинна перевірка ідентифікації

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

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, забезпечується шляхом перевірки удосконаленого електронного підпису, створеного за допомогою особистого ключа користувача на запиті на формування кваліфікованого сертифіката, за допомогою відкритого ключа, що міститься у цьому запиті, з використанням засобів кваліфікованого електронного підпису чи печатки Надавача.

Підтвердження володіння користувачем особистим ключем здійснюється без розкриття особистого ключа.

3.2.2. Автентифікація особи

Відповідно до вимог статті 22 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» під час формування кваліфікованого сертифіката відкритого ключа Надавач здійснює встановлення (ідентифікацію) особи заявника. Формування та видача кваліфікованого сертифіката відкритого ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті відкритого ключа, не допускаються.

Ідентифікація фізичної особи, фізичної особи - підприємця чи уповноваженого представника юридичної особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, здійснюється в один із таких способів:

1) за особистої присутності у приміщенні Надавача або ВПР - за паспортом громадянина України (в тому числі за е-паспортом або е-паспортом для виїзду за кордон, які надаються для

перевірки через мобільний застосунок "Дія") або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до закону України "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус". Для перевірки чинності документів, що посвідчують особу, за наявності технічної можливості використовується сервіс "Перевірка за базою недійсних документів" (https://dmsu.gov.ua/services/nd.html);

2) віддалено (без особистої присутності особи) - з використанням мобільного застосунку "Дія" (Договір про підключення до Єдиного державного вебпорталу електронних послуг від 07.03.2024 р.);

3) за ідентифікаційними даними особи, що містяться у кваліфікованому сертифікаті відкритого ключа електронного підпису чи печатки, раніше сформованого Надавачем або іншим КНЕДП, за умови чинності такого сертифіката.

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

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

Ідентифікація іноземних юридичних осіб здійснюється за інформацією з торговельного, банківського, судового реєстрів, які ведуться країною резидентства іноземної юридичної особи, перелік яких розміщує на своєму офіційному веб-сайті центральний засвідчувальний орган, або за документом, виданим відповідно до законодавства іноземної держави, легалізованим (консульська легалізація чи проставлення апостиля) відповідно до законодавства у сфері легалізації офіційних документів, якщо інше не встановлено законом або міжнародними договорами України.

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

Надавач під час формування та видачі кваліфікованого сертифіката відкритого ключа електронної печатки юридичної особи здійснює ідентифікацію особи уповноваженого представника юридичної особи, а також перевіряє обсяг його повноважень за документом, що визначає повноваження уповноваженого представника юридичної особи, чи з використанням інформації, що міститься в ЄДР або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи.

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

Перелік документів, необхідних для отримання кваліфікованих сертифікатів відкритих ключів електронного підпису чи печатки юридичними та фізичними особами, визначається розпорядчим документом Надавача та публікується на загальнодоступному інформаційному ресурсі Надавача.

У випадках передачі обслуговування кваліфікованих сертифікатів користувачів та документованої інформації, на підставі якої були сформовані зазначені сертифікати, від надавача, який припиняє свою діяльність, до Надавача, процедура ідентифікації цих користувачів проводиться одним із способів зазначених в цьому пункті та відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Відповідні Положення сертифікаційних практик Надавача містять додаткову інформацію.

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

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

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

Відповідні Положення сертифікаційних практик Надавача містять додаткову інформацію.

3.3. Ідентифікація та автентифікація при повторному формуванні кваліфікованих сертифікатів відкритого ключа

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

3.3.1. Ідентифікація та автентифікація користувача при повторному формуванні сертифіката за умови чинності попереднього сертифіката

Для формування нового кваліфікованого сертифіката користувача, що має чинний кваліфікований сертифікат, сформований Надавачем, такий користувач проходить процедуру автентифікації за поданою в електронній формі до Надавача заявою про формування кваліфікованого сертифіката за умови незмінності ідентифікаційних даних, внесених до попереднього кваліфікованого сертифіката, з моменту формування кваліфікованого сертифіката до моменту створення кваліфікованого електронного підпису на заяві про формування кваліфікованого сертифіката.

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

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

3.3.2. Ідентифікація та автентифікація користувача при повторному формуванні кваліфікованого сертифіката відкритого ключа у разі скасування сертифіката

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

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

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

Заява про скасування (блокування, поновлення) кваліфікованого сертифіката електронного підпису чи печатки подається Надавачеві у спосіб, що забезпечує підтвердження особи користувача.

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

4. ВИМОГИ ДО ЖИТТЄВОГО ЦИКЛУ СЕРТИФІКАТА

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

4.1. 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.

Пункт 4.1 відповідних Положень сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містить додаткову інформацію щодо процесу реєстрації користувача.

4.2. Обробка запиту на сертифікат

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

Обробка запиту на формування кваліфікованого сертифіката здійснюється програмними засобами ІКС Надавача за участю адміністратора реєстрації, працівника відокремленого пункту реєстрації Надавача, на якого покладено обов'язки з реєстрації користувачів та який виконує функції адміністратора реєстрації, або автоматично. Автоматична обробка запитів не виключає процесів ідентифікації особи користувача та підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката.

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

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

4.3. Формування сертифіката

Надання сформованого кваліфікованого сертифіката користувачу може здійснюватись в один із таких способів:

- шляхом надсилання файлу із сформованим кваліфікованим сертифікатом на адресу електронної пошти, вказану користувачем;
- шляхом запису файлу із сформованим кваліфікованим сертифікатом на носій інформації, наданий користувачем;
- шляхом публікації сформованого кваліфікованого сертифіката на веб сайті Надавача.

4.4. Прийняття сертифіката

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

Кваліфікований сертифікат користувача публікується на вебсайті Надавача за посиланням https://uakey.com.ua після обробки запиту на сертифікат (за умови надання користувачем згоди на публікацію сертифіката).

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

У разі виявлення користувачем протягом однієї доби невідповідності ідентифікаційних даних, внесених Надавачем до кваліфікованого сертифіката, користувач повинен звернутися до Надавача для скасування кваліфікованого сертифіката та формування нового сертифіката.

4.5. Використання пари ключів і сертифіката

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

4.5.1. Використання особистого ключа та сертифіката користувачем

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

- забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;
- невідкладно повідомляти Надавача про підозру або факт компрометації особистого ключа;
- не використовувати особистий ключ у разі його компрометації, а також у разі скасування або блокування відповідного кваліфікованого сертифіката;
- особисто відповідати за захист паролю від особистого ключа.

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

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

- цієї Політики сертифіката;
- відповідних Положень сертифікаційних практик Надавача;
- Договору про надання кваліфікованих електронних довірчих послуг, укладеного з Надавачем.

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, зокрема шляхом перевірки та підтвердження електронного підпису чи печатки.

Перш ніж прийняти кваліфікований електронний підпис чи печатку користувача, суб’єкт, який довіряє Надавачу, повинен перевірити таку інформацію:

– статус кваліфікованого сертифіката користувача, сферу використання кваліфікованого сертифіката користувача, обмеження використання та інформацію про кваліфікований сертифікат користувача;

– відповідність особистого ключа кваліфікованого електронного підпису чи печатки відкритому ключу, зазначеному в кваліфікованому сертифікаті користувача.

Суб’єкт, який довіряє Надавачу, повинен виконати такі перевірки:

– перевірити статус кваліфікованого сертифіката користувача на момент накладання кваліфікованого електронного підпису чи печатки за допомогою OCSP-сервера Надавача (сервер перевірки статусу кваліфікованого сертифіката), сферу використання (поле KeyUsage в сертифікаті), обмеження використання та інформацію про кваліфікований сертифікат, щоб переконатися, що кваліфікований сертифікат користувача чинний в даний момент;

– перевірити статус кваліфікованого сертифіката Надавача на момент накладання кваліфікованого електронного підпису чи печатки користувачем.

Кваліфікований електронний підпис чи печатка вважаються дійсними, коли всі вищенаведені перевірки виконані успішно.

Під час використання відкритого ключа та кваліфікованого сертифіката користувача суб’єкти, які довіряють Надавачу, повинні дотримуватися вимог законодавства у сфері електронних довірчих послуг, а також положень:

– цієї Політики сертифіката;

– відповідних Положень сертифікаційних практик Надавача.

4.6. Поновлення сертифіката

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

Надавач зобов'язаний забезпечувати, зокрема:

– цілодобовий прийом та перевірку заяв в електронній формі користувачів про поновлення їхніх кваліфікованих сертифікатів;

– прийом та перевірку заяв у паперовій формі користувачів про поновлення їхніх кваліфікованих сертифікатів протягом одного робочого дня після надходження заяви та згідно з режимом роботи Надавача;

– поновлення кваліфікованих сертифікатів відповідно до вимог Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

4.7. Повторне формування сертифіката

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

Надавач здійснює формування кваліфікованого сертифіката користувача, в тому числі, на підставі чинного кваліфікованого сертифіката, що містить ідентифікаційні дані користувача, отримані за результатами його ідентифікації в один із таких способів:

- за особистої присутності фізичної особи, фізичної особи - підприємця чи уповноваженого представника юридичної особи - за результатами перевірки відомостей (даних) про особу, отриманими у встановленому законодавством порядку з ЄДДР, за паспортом громадянина України або іншими документами, виданими відповідно до законодавства про ЄДДР та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи;
- віддалено (без особистої присутності особи), з одночасним використанням засобу електронної ідентифікації, що має високий або середній рівень довіри, раніше виданого фізичній особі, фізичній особі - підприємцю чи уповноваженому представнику юридичної особи за особистої присутності, та багатофакторної автентифікації.

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

Сформувати новий кваліфікований сертифікат користувач також може після скасування або закінчення строку дії сертифіката, звернувшись в офіс Надавача або відокремлений пункт реєстрації Надавача.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

4.8. Зміна сертифіката

Внесення змін до кваліфікованого сертифіката не допускається.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

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 та ДСТУ ETSI EN 319 411-2.

Надавач зобов'язаний забезпечувати, зокрема:

- цілодобовий прийом та перевірку заяв в електронній формі користувачів про скасування та блокування їхніх кваліфікованих сертифікатів, сформованих Надавачем;
- прийом та перевірку заяв у паперовій формі користувачів про скасування та блокування їхніх кваліфікованих сертифікатів, сформованих Надавачем, протягом одного робочого дня після надходження заяви та згідно з режимом роботи Надавача;
- скасування та блокування кваліфікованих сертифікатів, сформованих Надавачем, відповідно до вимог Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

Користувач має право за власним бажанням здійснити скасування кваліфікованого сертифіката шляхом подання заяви в паперовій або електронній формі.

Користувач має право за власним бажанням здійснити блокування кваліфікованого сертифіката. Блокування кваліфікованого сертифіката може здійснюватись Надавачем за заявою в паперовій або електронній формі або після ідентифікації користувача за ключовою фразою голосової автентифікації, первинний обмін якою між користувачем та Надавачем здійснюється під час подання заяви про формування кваліфікованого сертифіката відкритого ключа. Під блокуванням кваліфікованого сертифіката розуміється тимчасове призупинення чинності кваліфікованого сертифіката.

Після блокування кваліфікованого сертифіката, користувач може поновити чинність кваліфікованого сертифіката шляхом подання заяви в паперовій або електронній формі.

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.

Відповідні Положення сертифікаційних практик Надавача містять додаткову інформацію.

4.10. Служби статусу сертифіката

Надавач забезпечує доступність інформації про статус сертифіката в реальному часі за допомогою OCSP-серверу та списків відкликаних сертифікатів (CRL), що публікуються на веб-сайті 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 319 411-1:2022

Крім того, застосовуються такі особливі вимоги:

5.1.1. Вимоги до приміщень Надавача

Приміщення Надавача повинні бути розділені на функціональні зони за рівнями безпеки приміщень, встановленими Надавачем.

Приміщення Надавача за рівнями безпеки поділяються на спеціальні та службові. Для кожного рівня безпеки приміщень визначається мінімально необхідний набір механізмів безпеки, зокрема: контролю доступу, виявлення вторгнень, пожежної сигналізації та пожежогасіння, альтернативних та резервних джерел електроживлення тощо.

Зазначені механізми безпеки приміщень можуть бути змінені на підставі оцінених ризиків та відповідних цим ризикам обраних механізмів їх нейтралізації.

Компоненти, які є критичними для безпечної роботи Надавача, мають розташовуватися в захищеному та безпечному середовищі з фізичним захистом від вторгнення.

5.1.2. Фізичний доступ

Доступ до спеціальних та службових приміщень Надавача (безпечна зона) забезпечується із застосуванням організаційно-технічних заходів контролю (фізичний та логічний контроль) відповідно до внутрішніх організаційно-розпорядчих документів Надавача.

Право доступу до спеціальних приміщень мають право тільки керівник Надавача та персонал Надавача відповідно до своїх службових обов'язків, які внесені у відповідний перелік авторизованих співробітників Надавача, що мають доступ до спеціальних приміщень Надавача.

Доступ не авторизованих співробітників до спеціальних приміщень здійснюється виключно в супроводі керівника Надавача або адміністратора безпеки.

5.2. Процедурний контроль

Процедурний контроль здійснюється відповідно до вимог, визначених в пункті 6.4.3 ДСТУ ETSI EN 319 401.

5.3. Контроль персоналу

Контроль персоналу здійснюється відповідно до вимог, визначених в пункті 6.4.4 ДСТУ ETSI EN 319 401, а також відповідно до посадових інструкцій персоналу та внутрішньої документації КСЗІ в 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 КНЕДП ТОВ «Центр сертифікації ключів «Україна»" (для відокремлених пунктів реєстрації Надавача, що працюють за договором представництва);
- 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.

Адміністратори реєстрації відповідають за виконання функцій та несуть обов’язки адміністратора реєстрації, визначені у цій Політиці сертифіката.

З числа адміністраторів реєстрації на відокремленому пункті реєстрації призначаються відповідальні за захист інформації.

В межах виконання своїх обов'язків відповідальний за захист інформації на відокремленому пункті реєстрації відповідає за належну експлуатацію комплексу засобів захисту відокремленого пункту реєстрації.

Основними обов'язками відповідального за захист інформації на відокремленому пункті реєстрації є:

- організація експлуатації та технічного обслуговування апаратних та програмних засобів відокремленого пункту реєстрації;
- участь у впровадженні та забезпеченні функціонування КСЗІ в ІКС відокремленого пункту реєстрації;
- контроль за використанням особистих ключів персоналу відокремленого пункту реєстрації;
- участь у створенні та введенні в експлуатацію відокремленого пункту реєстрації.

Допускається виконання функцій відповідального за захист інформації на відокремленому пункті реєстрації системним адміністратором та адміністратором безпеки Надавача у частині, що не суперечить їхнім аналогічним функціям по відношенню до інших складових ІКС Надавача.

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 та ДСТУ ETSI EN 319 411-2.

5.4.1. Типи записаних подій

Процедури з управління доказами та архівами повинні передбачати ведення журналів аудиту подій, у яких реєструються події таких типів:

- спроби створення, знищення, встановлення паролів, зміни прав доступу в ІКС Надавача тощо;
- заміна технічних засобів ІКС Надавача та пар ключів;
- формування, блокування, скасування та поновлення сертифікатів, формування списків відкликаних сертифікатів (CRL);
- спроби несанкціонованого доступу до ІКС Надавача;
- надання доступу персоналу до ІКС Надавача;
- зміни системних конфігурацій та технічне обслуговування ІКС Надавача;
- збої в роботі ІКС Надавача;
- інші події, необхідні для збору доказів.

5.4.2. Частота обробки журналу аудиту подій

Журнали аудиту подій резервуються та переглядаються адміністратором безпеки не рідше одного разу на тиждень, в рамках чого перевіряється наявність несанкціонованої модифікації та вивчаються події.

5.4.3. Строки зберігання журналу аудиту подій

Надавач зберігає журнали аудиту подій протягом 10 років.

5.4.4 Захист журналу аудиту подій

Усі записи в журналах аудиту подій в електронній 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 журналу аудиту подій здійснюється Надавачем відповідно до внутрішньої документації КСЗІ в ІКС Надавача.

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 та ДСТУ ETSI EN 319 411-2.

5.5.1. Види документів та даних, що підлягають архівному зберіганню

Архівне зберігання інформації здійснюється згідно із внутрішніми організаційно-розпорядчими документами Надавача.

Обов'язковому архівуванню підлягають:

- кваліфіковані сертифікати Надавача та користувачів;
- списки відкликаних сертифікатів (CRL);
- журнали аудиту подій;
- документована інформація - документи (заяви на формування, блокування, поновлення, скасування сертифікатів користувачів), на підставі яких користувачам надавалися електронні довірчі послуги.

5.5.2. Строки зберігання архіву

Документи в паперовій та електронній формах мають зберігатися в порядку, встановленому законодавством у сфері архівної справи та законодавства у сфері електронних довірчих послуг.

Сертифікати Надавача, сертифікати серверів Надавача та сертифікати адміністраторів, сертифікати користувачів, а також списки відкликаних сертифікатів (CRL) зберігаються постійно.

5.5.3. Захист архіву

Надавач забезпечує захист архіву згідно із внутрішніми організаційно-розпорядчими документами та законодавством у сфері архівної справи.

Архівне приміщення обладнується технічними засобами, які виключають можливість проникнення сторонніх осіб та неконтрольованого доступу до інформації, що підлягає архівуванню.

5.5.4. Процедури резервного копіювання архіву

Надавач забезпечує резервне копіювання архіву згідно із вимогами та інструкціями на ІКС Надавача.

Засоби, що входять до складу центрального вузла ІКС Надавача, забезпечують автоматичне резервне копіювання даних. Автоматичне створення резервної копії має виконуватися не рідше одного разу на добу під час найменшого завантаження ресурсів ІКС Надавача.

Додатково може виконуватися резервне копіювання сертифікатів на оптичні носії або інші з'ємні носії інформації в ручному режимі. Після створення нової резервної копії попередня стає архівною.

Відновлення даних із резервної копії здійснюється засобами ІКС Надавача шляхом зчитування даних з останньої (актуальної) резервної копії та запису їх у базу даних ІКС Надавача.

Резервні копії баз даних та журнали аудиту подій зберігаються у приміщенні ІКС Надавача протягом 10 років. Контроль за здійсненням автоматичного резервного копіювання та виконання резервного копіювання в ручному режимі покладаються на системного адміністратора. Адміністратор безпеки регулярно 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 5.2.1 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 пари ключів Надавача та серверів ІКС Надавача може бути:

- планова;
- позапланова.

Планова зміна пари ключів Надавача виконується не пізніше ніж за два роки до завершення строку дії кваліфікованого сертифіката Надавача для забезпечення безперебійної роботи Надавача та кваліфікованих сертифікатів користувачів.

Процедура планової зміни ключів Надавача виконується у спеціальному приміщенні за участі керівника Надавача або адміністратора безпеки та адміністратора сертифікації.

Після генерації нового особистого та відкритого ключа та формування запиту на кваліфікований сертифікат відкритого ключа керівник Надавача ініціює процес засвідчення чинності відкритого ключа Надавача в центральному засвідчувальному органі відповідно до Регламенту роботи центрального засвідчувального органу, затвердженого наказом Міністерства цифрової трансформації України від 28 лютого 2024 р. № 33, зареєстрованого в Міністерстві юстиції України 15 березня 2024 р. за № 393/41738.

Після отримання кваліфікованого сертифіката відкритого ключа Надавача від центрального засвідчувального органу новий сертифікат Надавача публікується на офіційному веб-сайті Надавача, поточна пара ключів Надавача стає попередньою, а нова згенерована пара ключів стає поточною.

Попередній особистий ключ Надавача використовується тільки для створення кваліфікованої електронної печатки Надавача на даних щодо статусу кваліфікованих сертифікатів відкритих ключів підписувачів та створювачів електронних печаток, сформованих до планової зміни ключів Надавача. Попередній відкритий ключ Надавача використовується для перевірки кваліфікованої електронної печатки на кваліфікованих сертифікатів відкритих ключів підписувачів та створювачів електронних печаток, сформованих до планової зміни ключів Надавача, та кваліфікованої електронної печатки на даних щодо статусу цих сертифікатів.

Після завершення строку чинності кваліфікованого сертифіката попереднього відкритого ключа Надавача відповідний особистий ключ та всі його копії знищуються.

Попередній відкритий ключ Надавача зберігається у кваліфікованому сертифікаті відкритого ключа Надавача постійно.

Позапланова зміна пари ключів виконується у випадках компрометації або підозри на компрометацію особистих ключів Надавача (серверів ІКС Надавача) або у разі виходу з ладу ЗКЕП (криптомодуля) з особистим ключем і неможливості відновлення ключів з резервної копії.

Після зміни особистих ключів Надавач формує кваліфіковані сертифікати користувачів з використанням нової пари ключів Надавача.

Доступ до актуального кваліфікованого сертифіката Надавача забезпечено на офіційному веб-сайті ЦЗО за посиланням: https://czo.gov.ua/ca-registry-details?type=0&id=96.

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 та ДСТУ ETSI EN 319 411-2 .

5.7.1. Процедури обробки інцидентів і компрометації

Надавач має план реагування на інциденти та план відновлення після аварій.

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 відновлення ресурсів ІКС 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 центрального вузла 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 та ДСТУ ETSI EN 319 411-2. 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 кваліфікованих електронних довірчих послуг.

У разі відмови користувача від продовження отримання послуг за договором про надання кваліфікованих 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 кваліфікованих 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 кваліфікованих 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 кваліфікованих 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 та ДСТУ ETSI EN 319 411-2.

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, ДСТУ ETSI EN 319 411-2.

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 та серверів Надавача виконується у криптографічному модулі (далі - криптомодуль) у складі центрального вузла ІКС Надавача, який знаходиться у спеціальному приміщенні, двома особами – керівником Надавача або адміністратором безпеки та адміністратором сертифікації.

Перед процесом генерації особистого ключа здійснюється автентифікація адміністратора сертифікації у криптомодулі. Дані автентифікації у криптомодулі створюються згідно з експлуатаційною документацією на криптомодуль до початку процесу генерації.

Генерація особистих ключів та відповідних їм відкритих ключів Надавача здійснюється згідно з експлуатаційною документацією на відповідний ЗКЕП ІКС Надавача, на якому здійснюється генерація.

6.1.1.2. Генерація пари ключів користувача

Під час надання кваліфікованої електронної довірчої послуги із створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток Надавачем забезпечується:

- використання користувачем виключно засобу кваліфікованого електронного підпису чи печатки;
- захист обміну інформацією між користувачем та Надавачем засобами електронних комунікаційних мереж загального користування;
- створення умов для генерації пари ключів користувача;
- допомога під час генерації пари ключів користувача у спосіб, що не допускає порушення конфіденційності та цілісності особистого ключа, а також ознайомлення із значенням параметрів особистого ключа та їх копіювання;
- унікальність пари ключів користувача;
- зберігання особистого ключа користувача;
- захист від доступу сторонніх осіб до параметрів особистого ключа користувача під час використання засобу кваліфікованого електронного підпису чи печатки.

Особистий ключ у складі пари ключів користувача може бути згенерований:

- на стаціонарному робочому місці користувача або на власному портативному обчислювальному пристрої;
- на робочій станції в офісі Надавача та відокремлених пунктів реєстрації Надавача.

У разі коли пара ключів була згенерована користувачем поза приміщенням Надавача та/або за відсутності відповідного персоналу, ідентифікація такого користувача, перевірка достатності обсягу його цивільної правоздатності і дієздатності, формування та видача йому кваліфікованого сертифіката здійснюється Надавачем після перевірки факту володіння користувачем особистим ключем, який відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката.

Генерацію та/або управління парою ключів від імені користувача може здійснювати виключно Надавач. Під час управління парою ключів користувача Надавач може здійснювати резервне копіювання особистого ключа користувача з метою його зберігання за умови дотримання таких вимог:

- рівень безпеки резервної копії особистого ключа повинен відповідати рівню безпеки оригінального особистого ключа;

– кількість резервних копій не повинна перевищувати мінімального значення, необхідного для забезпечення безперервності послуги.

Для генерації особистих ключів використовуються засоби кваліфікованого електронного підпису чи печатки, які можуть функціонувати під управлінням або з використанням окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків та які перебувають у власності користувачів, або надаються Надавачем.

Згенерований особистий ключ користувача захищається за допомогою атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа (пароль, PIN-код, біометричні дані володільця особистого ключа тощо).

Для надання кваліфікованих електронних довірчих послуг Надавачем 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.

Надання Надавачем засобів кваліфікованого електронного підпису чи печатки у вигляді апаратно-програмних засобів та їх технічна підтримка і обслуговування здійснюється на договірних засадах.

Надання Надавачем засобів кваліфікованого електронного підпису чи печатки у вигляді окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків, може здійснюватись шляхом передачі цих засобів на носіях інформації безпосередньо користувачу або шляхом надання доступу через веб-сайт Надавача.

6.1.2. Доставка особистого ключа користувачу

Отримання користувачем особистого ключа у володіння в результаті надання Надавачем кваліфікованої електронної довірчої послуги здійснюється за таких умов:

– отримання та використання особистого ключа на правах повного володіння засобом кваліфікованого електронного підпису чи печатки, у тому числі, носієм особистого ключа;

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

Фактичне отримання користувачем особистого ключа відбувається у момент генерації особистого ключа особисто або у момент зміни атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа (пароль, PIN-код, біометричні дані володільця особистого ключа) у випадку, коли ключові пари були попередньо створено Надавачем. Не допускається формування Надавачем кваліфікованих сертифікатів до моменту фактичного отримання особистого ключа користувачем.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

6.1.3. Доставка відкритого ключа користувачу

Відкритий ключ надається для формування кваліфікованого сертифіката у складі запиту на формування кваліфікованого сертифіката, який являє собою файл формату PKCS#10, що

містить відкритий ключ користувача і додаткову інформацію для формування кваліфікованого сертифіката.

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

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

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

Контейнер ланцюжків сертифікатів, доступний для завантаження суб'єктами, які довіряють Надавачу, розміщений на веб-сайті Надавача за посиланням: http://uakey.com.ua/uakeycert.p7b.

Доступ до актуального кваліфікованого сертифіката Надавач забезпечено на офіційному веб-сайті ЦЗО за посиланням: https://czo.gov.ua/ca-registry-details?type=0&id=96.

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;
- алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);
- алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

6.1.6. Генерація параметрів відкритого ключа

Під час генерації відкритого ключа використовується апаратний генератор випадкових чисел (ГВЧ). Ключі генеруються та зберігаються в апаратно-програмному мережевому криптомодулі.

6.1.7. Основні цілі використання особистого ключа надавачем

Особисті ключі Надавача та серверів ІКС Надавача забезпечують функціонування ІКС Надавача.

Надавач використовує ключі Надавача для підпису сертифікатів користувачів, сертифікатів серверів ІКС 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 ЗКЕП, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами державної експертизи або сертифікації таких засобів, а також файлові контейнери формату PKCS#12.

Для зберігання особистих ключів Надавача та серверів ІКС Надавача використовуються мережні криптомодулі, що виконані у вигляді окремих апаратно-програмних 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 (адміністратори сертифікації) під контролем адміністратора безпеки.

Управління особистими ключами Надавача здійснюється посадовими особами після їх автентифікації в мережному криптомодулі за їх особистими атрибутами доступу.

6.2.3. Управління особистим ключем підписувача

Надавач забезпечує зберігання та захист особистих ключів користувачів, згенерованих в мережних криптомодулях, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами державної експертизи або сертифікації таких засобів, які розміщені в спеціальних приміщеннях Надавача, доступ до яких мають тільки відповідальні особи 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

Після скасування або завершення строку дії кваліфікованих сертифікатів користувачів особистий ключ користувача, що зберігається в мережному криптомодулі Надавача, автоматично знищується.

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 ІКС Надавача виконується на сервері ІКС Надавача у службовому приміщенні надавача адміністратором сертифікації.

Під час введення в дію особистого ключа шляхом підключення криптомодуля до серверів Надавача здійснюється автентифікація адміністратора сертифікації у криптомодулі.

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 ІКС Надавача відповідний особистий ключ та всі його резервні копії знищуються.

Знищення особистих ключів Надавача та серверів ІКС Надавача здійснюється згідно з експлуатаційною документацією на відповідні засоби кваліфікованого електронного підпису чи печатки, ЗКЕП чи мережні криптомодулі, 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 у складі відповідних сертифікатів.

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 ЗКЕП, 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.

6.6.2. Засоби керування безпекою

Контроль за дотриманням вимог з безпеки в ІКС Надавача здійснюється службою 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 Надавач 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 Надавача за допомогою ЗКЕП 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 та ДСТУ ETSI EN 319 411-2.

7.1. Профілі сертифікатів

Кваліфіковані сертифікати, 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» (далі - ISO/IEC 9594-8:2020).
- ДСТУ ETSI EN 319 412-1 (ETSI EN 319 412-1 V1.4.4, IDT) «Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 1. Огляд та типові структури даних» (далі - ДСТУ ETSI EN 319 412-1).
- ДСТУ ETSI EN 319 412-2 (ETSI EN 319 412-2, IDT) «Електронні підписи та інфраструктури. (ESI). Профілі сертифікатів. Частина 2. Профілі сертифікатів, виданих фізичним особам» (далі - ETSI EN 319 412-2).
- ДСТУ ETSI EN 319 412-3 (ETSI EN 319 412-3, IDT) «Електронні підписи та інфраструктури (ESI). Профілі сертифікатів. Частина 3. Профілі сертифікатів, виданих юридичним особам».
- ДСТУ ETSI EN 319 412-5 (ETSI EN 319 412-5, IDT) «Електронні підписи та інфраструктури. Профілі сертифікатів. Частина 5. Кваліфіковані сертифікати».
- ДСТУ ETSI TS 119 312 (ETSI TS 119 312, IDT) «Електронні підписи та інфраструктури (ESI). Криптографічні набори».
- ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння», (далі - ДСТУ 4145-2002). З функцією гешування за ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования» або за ДСТУ 7564-2014 «Інформаційні технології. Криптографічний захист інформації. Функція ґешування».

Поля та формат інформації, що міститься в кваліфікованому сертифікаті:

Найменування	**Значення**
Версія	Версія 3 стандарту X.509
Серійний номер	Номер сертифіката. Значення цього поля є унікальним.

Алгоритм підпису	Криптографічний алгоритм. Визначає алгоритм, який використовується для підпису кваліфікованого сертифіката.
Видавець	Назва надавача, що формує кваліфікований сертифікат
Дійсний від	Дата початку дії кваліфікованого сертифіката (відповідно до стандарту RFC 5280)
Дійсний до	Дата закінчення строку дії кваліфікованого сертифіката (відповідно до стандарту RFC 5280)
Суб'єкт	Інформація про отримувача кваліфікованого сертифіката (відповідно до стандарту RFC 5280) Детальніше див. п. 3.1.1
Відкритий ключ	Відкритий ключ, що відповідає особистому ключу кваліфікованого сертифіката (відповідно до стандарту RFC 5280)
Підпис	Кваліфікований електронний підпис Надавача, що надає послугу створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки. Згенерований та закодований відповідно до стандарту RFC 5280.

7.2. Профілі списку відкликаних сертифікатів (CRL)

Списки відкликаних сертифікатів (CRL), що формуються Надавач повинні відповідати вимогам таких стандартів:

- ДСТУ ISO/IEC 9594-8:2021 (ISO/IEC 9594-8:2020, IDT) «Інформаційні технології. Взаємозв'язок відкритих систем. Частина 8. Каталог. Структура сертифікатів відкритих ключів та атрибутів» (далі - ISO/IEC 9594-8:2020).
- RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile».

Формат інформації в CRL, що публікується Надавач, відповідає стандарту ITU-T X.509 та регламенту RFC 5280. CRL повинен мати щонайменше такі поля:

Найменування	**Значення**
Версія	Версія CRL (2)
Видавець	Назва Надавача, що формує CRL

Дата набрання чинності	Поточна дата випуску (оновлення) CRL
Наступне оновлення	Дата наступного оновлення CRL
Відкликані сертифікати	У цьому полі міститься інформація про відкликані кваліфіковані сертифікати, зокрема: - серійний номер відкликаного кваліфікованого сертифіката; - дата зміни статусу; - код причини зміни статусу.
Алгоритм підпису	Алгоритм, що використовується для підписання CRL
Підпис	Значення електронного підпису Надавача
Розширення CRL	Інша розширена інформація (необов'язкові поля)

7.3. Профілі протоколу визначення статусу сертифіката (OCSP)

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

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

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

- ISO/IEC 8825-1:2002 «Information technology - ASN.1 Encoding Rules - Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER);
- RFC 2560 «Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP».

8. АУДИТ ВІДПОВІДНОСТІ ТА ІНШІ ОЦІНКИ

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

8.1. Частота або обставини оцінювання

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

- вимагає від Надавача усунення порушень вимог законодавства у сфері електронних довірчих послуг у встановлений приписом строк;
- приймає рішення про блокування кваліфікованого сертифіката Надавача, якщо під час перевірки виникла підозра компрометації особистого ключа;

- приймає рішення про скасування кваліфікованого сертифіката Надавача, якщо під час перевірки виявлено факт компрометації особистого ключа;
- 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;
    - неусунення 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;
– 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 надавачі повинні 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

Надавач контролює дотримання цієї Політики сертифіката та відповідних Положень сертифікаційних практик, суворо контролюючи якість своїх послуг та 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 та ДСТУ ETSI EN 319 411-2.

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 Надавача, опублікованими на веб-сайті Надавача.

У разі надання кваліфікованих електронних довірчих послуг через відокремлені пункти реєстрації Надавача може стягуватися додаткова плата за надання кваліфікованих електронних довірчих послуг.

Поновлення заблокованих кваліфікованих сертифікатів здійснюється на безоплатній основі.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 2 до цього Регламенту) містять додаткову інформацію.

9.1.2. Плата за доступ до сертифіката

Немає плати за доступ до кваліфікованого сертифіката.

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;
- зберігання особистих ключів в хмарному сховищі Надавача.

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

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.

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

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 «Центр сертифікації ключів «Україна»), 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 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 та 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 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 (ТОВ «Центр сертифікації ключів «Україна») 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.

Додаток 2
до Регламенту роботи кваліфікованого
надавача електронних довірчих послуг
ТОВ «Центр сертифікації ключів «Україна»

ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ ТОВ «ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ «УКРАЇНА»

Зміст

3.1.5. Унікальність позначень сертифіката

3.1.6. Визнання, автентифікація та роль торгових марок

3.2. Первинна перевірка ідентифікації

3.2.1. Метод підтвердження володіння особистим ключем

3.2.2. Автентифікація особи

3.2.3. Неперевірена інформація про користувача

3.2.4. Підтвердження повноважень

3.3. Ідентифікація та автентифікація під час повторного формування сертифіката

3.4. Ідентифікація та автентифікація користувача під час блокування або скасування сертифіката

3.5. Автентифікація при втраті засобу автентифікації

4. Вимоги до життєвого циклу сертифіката

4.1. Запит на формування сертифіката

4.2. Обробка заяви на формування сертифіката

4.3. Видача сертифіката

4.4. Прийняття сертифіката

4.5. Використання пари ключів і сертифіката

4.5.1. Використання особистого ключа та сертифіката користувачем

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

4.6. Поновлення сертифіката

4.7. Повторне формування сертифіката

4.8. Зміна сертифіката

4.9. Блокування та скасування сертифіката

4.10. Послуга перевірки статусу сертифіката

4.11. Закінчення строку дії сертифіката

4.12. Депонування та повернення ключів

5. Об'єкт, управління та операційний контроль

5.1. Контроль фізичної безпеки

5.2. Процедурний контроль

5.3. Контроль персоналу

5.4. Ведення журналу аудиту подій

5.5. Архів документів

5.6. Зміна ключа

5.7. Компрометація і аварійне відновлення

5.8. Припинення діяльності надавача

6. Технічні заходи безпеки

6.1. Генерація та встановлення пари ключів

6.2. Захист особистого ключа та інженерний контроль криптографічного модуля

6.3. Інші аспекти керування парами ключів

6.4. Дані активації

6.5. Контроль комп'ютерної безпеки

6.6. Контроль безпеки життєвого циклу

6.7. Контроль безпеки мережі

6.8. Електронні позначки часу

7. Профілі сертифікатів, списків відкликаних сертифікатів та протоколу визначення статусу сертифіката

7.1. Профілі сертифікатів

7.2. Профілі списку відкликаних сертифікатів

7.3. Профілі протоколу визначення статусу сертифіката

8. Аудит відповідності та інші оцінки

8.1. Частота або обставини оцінювання

8.2. Особа/кваліфікація оцінювача

8.3. Відносини експерта з об’єктом оцінки

8.4. Теми, охоплені оцінюванням

8.5. Дії, вжиті внаслідок порушення

8.6. Повідомлення результатів

8.7. Самоперевірки

9. Інші комерційні та юридичні питання

9.1. Ціни і тарифи

9.1.1. Плата за видачу або поновлення сертифіката

9.1.2. Плата за доступ до сертифіката

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

9.1.4. Плата за інші послуги

9.1.5. Політика відшкодування

9.2. Фінансова відповідальність

9.3. Конфіденційність ділових даних

9.4. Захист персональних даних

9.5. Права інтелектуальної власності

9.6. Заяви та гарантії

9.7. Відмова від відповідальності

9.8. Обмеження відповідальності

9.9. Збитки

9.10. Термін дії та припинення дії

9.11. Індивідуальні комунікації та угоди з суб’єктами інфраструктури відкритих ключів

9.12. 9.12. Зміни

9.13. Положення щодо вирішення спорів

9.14. Застосовне право

9.15. Дотримання чинного законодавства

1. ВСТУП

1.1. Огляд

Ці Положення сертифікаційних практик визначають перелік практичних дій та процедур щодо кваліфікованих сертифікатів електронного підпису та печатки (далі - кваліфіковані сертифікати) користувачів електронних довірчих послуг, зокрема, підписувачів та створювачів електронних печаток (далі - користувачі), які застосовуються Надавачем для реалізації Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Дотримання практичних дій та процедур, визначених у цих Положеннях сертифікаційних практик, є обов'язковим для керівника Надавача та найманих працівників Надавач, посадові обов'язки яких безпосередньо пов'язані з реєстрацією користувачів, формуванням та обслуговуванню їхніх кваліфікованих сертифікатів електронного підпису та печатки (далі - персонал), а також фізичних та юридичних осіб, які на підставі договорів, укладених з Надавачем (ТОВ «Центр сертифікації ключів «Україна») безпосередньо чи опосередковано пов'язані з реєстрацією користувачів, формуванням та/або обслуговуванням їхніх кваліфікованих сертифікатів електронного підпису та печатки, зокрема, відокремлених пунктів реєстрації Надавача.

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

Перелік усіх правил, що застосовуються Надавачем у процесі реєстрації користувачів, формування та обслуговування кваліфікованих сертифікатів відкритих ключів Надавача та користувачів, зокрема управління їх статусом (блокування, поновлення та скасування) визначається Політикою сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

Ці Положення сертифікаційних практик відповідають вимогам, визначеним у:

- ДСТУ ETSI EN 319 411-1 (ETSI EN 319 411-1 V1.3.1, IDT) «Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги» (далі -ДСТУ ETSI EN 319 411-1);
- ДСТУ ETSI EN 319 411-2 (ETSI EN 319 411-2 V2.4.1, IDT) «Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 2. Вимоги для надавачів довірчих послуг, які видають кваліфіковані сертифікати ЄС» (далі - ДСТУ ETSI EN 319 411-2).

1.2. Назва документа та його ідентифікація

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

Назва документа: Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна». Версія: 1.0.

1.3. Учасники інфраструктури відкритих ключів

Учасники інфраструктури відкритих ключів зазначені в пункту 5.4 ДСТУ ETSI EN 319 4111 та ДСТУ ETSI EN 319 411-2.

1.3.1. Надавач

Надавач 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, формування та обслуговування їхніх кваліфікованих сертифікатів, в тому числі, управління їхнім статусом (блокування, поновлення та скасування).

Надавач здійснює реєстрацію користувачів самостійно та/або через відокремлені пункти реєстрації Надавача.

Пункт 1.3.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить додаткову інформацію.

1.3.2. Органи реєстрації

Відокремлені пункти реєстрації Надавача є органами реєстрації, що представлені окремими підрозділами Надавача або юридичними чи фізичними особами, які на підставі договору з Надавачем здійснюють реєстрацію користувачів.

Безпосередню реєстрацію користувача у відокремленому пункті реєстрації Надавача здійснює працівник відокремленого пункту реєстрації, на якого покладено відповідні обов'язки з реєстрації користувачів (далі - віддалений адміністратор реєстрації).

До працівників відокремлених пунктів реєстрації Надавача, на яких покладено обов'язки з реєстрації користувачів, застосовуються такі ж вимоги, як і до адміністраторів реєстрації, що визначені у пункті 5.3.1.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

1.3.3. Користувачі

Користувачами є підписувачі та створювачі електронних печаток, щодо яких Надавач здійснює їх реєстрацію (самостійно або через відокремлені пункти реєстрації Надавача), формування та обслуговування їхніх кваліфікованих сертифікатів, а саме:

- підписувачі:
    - фізичні особи - резиденти;
    - фізичні особи - нерезиденти;
    - самозайняті особи (нотаріуси, адвокати, арбітражні керуючі, приватні виконавці, тощо);
    - посадові особи (наймані працівники, підрядники тощо) юридичної особи, представництва юридичної особи - нерезидента, посадові особи юридичної особи - нерезидента, фізичної особи - підприємця, самозайнятої особи;
- створювачі електронних печаток:
    - юридичні особи - резиденти;
    - представництва юридичних осіб - нерезидентів;
    - фізичні особи - підприємці.

Політика сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить додаткову інформацію.

1.3.4. Суб'єкти, які довіряють

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

Політика сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить додаткову інформацію.

1.4. Використання сертифіката

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

1.4.1. Дозволене використання сертифіката

Кваліфіковані сертифікати, сформовані Надавачем, дозволено використовувати для:

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

Надавач для визначення сфери використання кваліфікованого сертифіката користувача під час його формування встановлює розширення сертифіката «Призначення відкритого ключа» («keyUsage»), зазначені у Таблиці 1.

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

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

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

Надавач формує кваліфіковані сертифікати з розширеннями сертифіката «digitalSignature + nonRepudiation» або «keyAgreement» за умов, що такі відкриті ключі належать до різних ключових пар.

Надавач для визначення сфери використання кваліфікованого сертифіката користувача як кваліфікованого сертифіката електронної печатки під час його формування встановлює додаткове розширення «Уточнене призначення відкритого ключа» («extendedKeyUsage») із об’єктним ідентифікатором (OID): 1.2.804.2.1.1.1.3.9.

1.4.1.1. Види сертифікатів

Відповідно до цих Положень сертифікаційних практик Надавач формує кваліфіковані сертифікати таких типів:

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

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

1.4.2. Заборонене використання сертифіката

Не допускається використання кваліфікованого сертифіката, сформованого Надавачем, у сферах, які не відповідають зазначеному у кваліфікованому сертифікаті призначенню відкритого ключа («keyUsage»).

1.5. Управління Положеннями сертифікаційних практик

1.5.1. Відповідальність за Положення сертифікаційних практик

Ці Положення сертифікаційних практик підтримуються ТОВ «Центр сертифікації ключів «Україна». ТОВ «Центр сертифікації ключів «Україна» є зареєстрованою відповідно до законодавства юридичною особою.

Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені ТОВ «Центр сертифікації ключів «Україна» або від імені відокремленого пункту реєстрації Надавача.

Реквізити ТОВ «Центр сертифікації ключів «Україна»:

- Код згідно з Єдиним державним реєстром підприємств та організацій України (ЄДРПОУ): 36865753.
- Адреса: Україна, 03142, м. Київ, вул. Ірпінська, 1.
- Контактний телефон: +38 (044) 206-72-30.
- Адреса електронної пошти: info@uakey.com.ua.

Реквізити Надавача:

- Адреса веб-сайту: uakey.com.ua.
- Контактний телефон: +38 (044) 206-72-31.
- Адреса електронної пошти: info@uakey.com.ua.

Ці Положення сертифікаційних практик структуровані відповідно до RFC 3647 «Інфраструктура відкритих ключів Інтернету X.509 Політика сертифікатів і практика сертифікації» і містять всю необхідну інформацію.

Ці Положення сертифікаційних практик, а також зміни до них затверджуються директором ТОВ «Центр сертифікації ключів «Україна».

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

1.5.2. Внесення змін до Положень сертифікаційних практик

Відповідно до пункту 9.12 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

1.6. Визначення термінів та перелік скорочень

1.6.1. Визначення термінів

У цих Положеннях сертифікаційних практик терміни застосовуються у значеннях, наведених у Цивільному кодексі України, Законах України «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», «Про електронні комунікації», «Про електронну ідентифікацію та електронні довірчі послуги», постанові Кабінету Міністрів України від 28.06.2024 р. № 764 «Деякі питання дотримання вимог у сферах електронної ідентифікації та

електронних довірчих послуг», інших нормативно-правових актах у сферах електронних довірчих послуг, криптографічного та технічного захисту інформації, електронних комунікацій.

1.6.2. Перелік скорочень

ВПР	Відокремлений пункт реєстрації
ДРАЦС	Державний реєстр актів цивільного стану громадян
ДРФО	Державний реєстр фізичних осіб - платників податків
ЄДДР	Єдиний державний демографічний реєстр
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань
ЄДРПОУ	Єдиний державний реєстр підприємств та організацій України
ЄІС МВС	Єдина інформаційна система Міністерства внутрішніх справ України
ЗКЕП	Засіб кваліфікованого електронного підпису чи печатки
ІКС	Інформаційно-комунікаційна система
КЕП	Кваліфікований електронний підпис
КЗІ	Криптографічний захист інформації
КНЕДП	Кваліфікований надавач електронних довірчих послуг
КО	Контролюючий орган (Адміністрація державної служби спеціального зв'язку та захисту інформації України)
КСЗІ	Комплексна система захисту інформації
ООВ	Орган з оцінки відповідності
ОС	Операційна система
ПЗ	Програмне забезпечення
ПТК	Програмно-технічний комплекс - апаратно-програмні та програмні засоби, що забезпечують виконання функцій КНЕДП
РНОКПП	Реєстраційний номер облікової картки платника податків
ЦЗО	Центральний засвідчувальний орган (Міністерство цифрової трансформації України)

OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol

2. ОБОВ'ЯЗКИ ЩОДО ПУБЛІКАЦІЇ ТА ЗБЕРІГАННЯ

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

2.1. Репозиторій/вебсайт

Надавач через веб-сайт (https://uakey.com.ua) забезпечує вільний доступ до:

- відомостей про Надавача;
- даних про внесення відомостей про Надавача до Довірчого списку;
- Політики сертифіката Надавача;
- відповідних Положень сертифікаційних практик Надавача;
- загальних положень та умов надання кваліфікованих електронних довірчих послуг користувачам;
- кваліфікованих сертифікатів Надавача;
- переліку кваліфікованих електронних довірчих послуг, які надає Надавач;
- даних про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг Надавачем;
- форм документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;
- відомостей про відокремлені пункти реєстрації Надавача та виїзних адміністраторів реєстрації;
- реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів;
- відомостей про обмеження під час використання кваліфікованих сертифікатів користувачами;
- даних про порядок перевірки чинності кваліфікованого сертифіката, у тому числі умови перевірки статусу сертифіката;
- перелік актів законодавства у сфері електронних довірчих послуг.

Ці Положення сертифікаційних практик доступні 24 години на добу 7 днів на тиждень у форматі лише для читання на веб-сайті Надавача (https://uakey.com.ua).

2.2. Публікація інформації

2.2.1. Публікація сертифікатів користувачів

Адміністратор сертифікації Надавача забезпечує публікацію кваліфікованих сертифікатів користувачів, згода на публікацію яких надана такими користувачами, та списків відкликаних сертифікатів (CRL) на веб-сайті Надавача.

Надавач забезпечує вільний доступ до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів через власний веб-сайт.

2.2.2. Публікація сертифікатів надавача

Надавач забезпечує вільний доступ до інформації про кваліфіковані сертифікати Надавача через власний веб-сайт.

Відомості про кваліфіковані сертифікати Надавача, сформовані з використанням самопідписаного сертифіката електронної печатки центрального засвідчувального органу, статус та обмеження у використанні таких сертифікатів, а також списки відкликаних сертифікатів (CRL) містяться в реєстрі чинних, блокованих та скасованих сертифікатів відкритих ключів, що ведеться центральним засвідчувальним органом (https://czo.gov.ua/).

2.2.3. Доступ до сертифікатів користувачів

Надавач забезпечує цілодобовий доступ користувачів до їхніх власних кваліфікованих сертифікатів.

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

2.2.4. Строк закінчення дії сертифіката

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

Кваліфікований сертифікат вважається скасованим після настання дати та часу закінчення строку дії кваліфікованого сертифіката.

2.3. Час та періодичність публікації

Надавач формує списки відкликаних сертифікатів у вигляді повного та часткового списків, які відповідають таким вимогам:

- у кожному списку відкликаних сертифікатів зазначається граничний строк його дії до видання нового списку;
- новий список відкликаних сертифікатів може бути опубліковано до настання граничного строку його дії до видання наступного списку;
- на список відкликаних сертифікатів повинен бути накладений кваліфікований електронний підпис чи печатка Надавача.

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

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

Посилання на списки відкликаних сертифікатів вносяться до кваліфікованих сертифікатів користувачів.

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

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

2.4. Контроль доступу до репозиторію\веб-сайту

Кваліфіковані сертифікати Надавача та користувачів, списки відкликаних сертифікатів, відповідні Положення сертифікаційних практик та Політика сертифіката доступні у репозиторії\веб-сайті 24 години на добу 7 днів на тиждень.

Доступ лише для читання необмежений. Зміни у репозиторії\веб-сайті здійснюються виключно Надавачем.

Користувач може знайти інформацію про свій кваліфікований сертифікат шляхом здійснення його пошуку на веб-сайті Надавача.

3. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

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

3.1. Позначення

Кваліфіковані сертифікати, які формує Надавач, обов'язково повинні містити відомості, визначені частиною другою статті 23 Закону України "Про електронну ідентифікацію та електронні довірчі послуги", а саме:

- позначку (у формі, придатній для автоматизованої обробки) про те, що сертифікат виданий як кваліфікований сертифікат;
- позначку, що сертифікат виданий в Україні;
- ідентифікаційні дані, які однозначно визначають Надавача, у тому числі обов'язково найменування та код згідно з ЄДРПОУ;
- ідентифікаційні дані, які однозначно визначають користувача , у тому числі обов'язково:
    - прізвище, власне ім'я, по батькові (за наявності) підписувача та УНЗР або РНОКПП, або серію (за наявності) та номер паспорта громадянина України (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття РНОКПП та офіційно повідомили про це відповідний податковий орган і мають відмітку або інформацію в паспорті громадянина України про право здійснювати будь-які платежі за серією та/або номером паспорта), або номер паспортного документа іноземця чи особи без громадянства;
    - найменування або прізвище, власне ім'я, по батькові (за наявності) створювача електронної печатки та код згідно з ЄДРПОУ (код/номер з торговельного, банківського чи судового реєстру, що ведеться країною резидентства іноземної юридичної особи, код/номер з реєстраційного посвідчення місцевого органу влади іноземної держави про реєстрацію юридичної особи), крім міжнародних організацій, відомості про яких не внесені до ЄДР або торговельного, банківського чи судового реєстру, що ведеться іноземною державою, за місцезнаходженням штаб-квартири міжнародної організації, або унікальний номер запису в ЄДДР, або РНОКПП, або серію (за наявності) та номер паспорта громадянина України (для фізичних осіб, які через свої релігійні переконання

відмовляються від прийняття РНОКПП та офіційно повідомили про це відповідний податковий орган і мають відмітку або інформацію в паспорті громадянина України про право здійснювати будь-які платежі за серією та/або номером паспорта);

- значення відкритого ключа, який відповідає особистому ключу;
- відомості про початок та закінчення строку дії кваліфікованого сертифіката;
- серійний номер кваліфікованого сертифіката, унікальний для Надавача;
- кваліфікований електронний підпис або кваліфіковану електронну печатку, створені Надавачем;
- відомості про місце розміщення в безоплатному доступі кваліфікованого сертифіката, з використанням якого перевіряється удосконалений електронний підпис чи печатка, передбачені підпунктом 8 цього пункту;
- відомості про місце надання послуги перевірки статусу відповідного кваліфікованого сертифіката;
- зазначення про те, що особистий ключ, пов'язаний з відкритим ключем, зберігається в засобі кваліфікованого електронного підпису чи печатки, у формі, придатній для автоматизованої обробки.

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 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

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

Таблиця 2. Позначення, що використовуються в кваліфікованих сертифікатах користувачів

Найменування	**Значення**
Country (C)	Назва країни відповідно до ДСТУ ISO 3166-1:2009 «Коди назв країн світу» (ISO 3166-1:2006, IDT), затвердженого наказом Державного комітету України з питань технічного регулювання та споживчої політики від 23 грудня 2009 р. № 471
Organization (O)	Найменування юридичної особи для кваліфікованого сертифіката юридичної особи або кваліфікованого сертифіката представника юридичної особи.

Organizational Unit (OU)	Назва підрозділу або відділу в організації.
State or Province (S)	Назва області місцезнаходження або місця реєстрації користувача
Locality (L)	Назва міста місцезнаходження або місця реєстрації користувача
Common Name (CN)	Повне ім’я (найменування) користувача, якому належить кваліфікований сертифікат
E-Mail Address (E)	Електронна пошта користувача, якому належить кваліфікований сертифікат
Title (T)	Посада (для кваліфікованих сертифікатів представників юридичної особи за необхідності)

3.1.1. Типи позначень сертифіката

Типи позначень (реквізитів, атрибутів) кваліфікованого сертифіката, що відповідають відомостям, які містяться в кваліфікованих сертифікатах, визначені в стандартах щодо профілів сертифікатів відповідно до пункту 7.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

3.1.2. Позначення (реквізити та атрибути) сертифікатів

Кваліфікований сертифікат повинен мати всі необхідні позначення (реквізити, атрибути), визначені в стандартах щодо профілів сертифікатів відповідно до пункту 7.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

3.1.3. Анонімність або використання псевдонімів

Використання псевдонімів здійснюється відповідно до пункту 3.1.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту).

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 гарантувати, що сертифікати з однаковими даними, зазначеними в полях «Common Name» та «SerialNumber», не видаються різним користувачам.

3.1.6. Визнання, автентифікація та роль торгових марок

Не застосовується.

3.2. Первинна перевірка ідентифікації

3.2.1. Метод підтвердження володіння особистим ключем

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

3.2.2. Автентифікація особи

Формування та видача кваліфікованого сертифіката відкритого ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті відкритого ключа, не допускаються. Для ідентифікації користувача, що звернувся до Надавача для отримання кваліфікованих електронних довірчих послуг, Надавач вимагає разом із заявою надати, а користувач надає ідентифікаційні дані, які вносяться до кваліфікованого сертифіката.

Ідентифікація фізичної особи, фізичної особи - підприємця чи уповноваженого представника юридичної особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, здійснюється в один із таких способів:

1) за особистої присутності у приміщенні Надавача або ВПР - за паспортом громадянина України (в тому числі за е-паспортом або е-паспортом для виїзду за кордон, які надаються для перевірки через мобільний застосунок "Дія") або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до закону України "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус". Для перевірки чинності документів, що посвідчують особу, за наявності технічної можливості використовується сервіс "Перевірка за базою недійсних документів" (https://dmsu.gov.ua/services/nd.html);

2) віддалено (без особистої присутності особи) - з використанням мобільного застосунку "Дія";

3) за ідентифікаційними даними особи, що містяться у кваліфікованому сертифікаті відкритого ключа електронного підпису чи печатки, раніше сформованого Надавачем або іншим КНЕДП, за умови чинності такого сертифіката.

Під час перевірки цивільної правоздатності та дієздатності юридичної особи (з метою формування кваліфікованого сертифіката електронної печатки) чи фізичної особи - підприємця (з метою формування кваліфікованого сертифіката електронної печатки) Надавач зобов’язаний використовувати інформацію про юридичну особу чи фізичну особу - підприємця, що міститься в ЄДР, а також пересвідчитися, що обсяг цивільної правоздатності та дієздатності юридичної особи чи фізичної особи - підприємця є достатнім для формування та видачі кваліфікованого сертифіката відкритого ключа.

Ідентифікація іноземних юридичних осіб здійснюється за інформацією з торговельного, банківського, судового реєстрів, які ведуться країною резидентства іноземної юридичної особи, перелік яких розміщує на своєму офіційному веб-сайті центральний засвідчувальний орган, або за документом, виданим відповідно до законодавства іноземної держави, легалізованим (консульська легалізація чи проставлення апостиля) відповідно до законодавства у сфері легалізації офіційних документів, якщо інше не встановлено законом або міжнародними договорами України.

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

Перелік документів, необхідних для отримання кваліфікованих сертифікатів відкритих ключів електронного підпису чи печатки юридичними та фізичними особами, визначається розпорядчим документом Надавача та публікується на загальнодоступному інформаційному ресурсі Надавача.

3.2.2.1. Порядок ідентифікації та автентифікації при особистому зверненні заявника

У випадку особистого звернення заявника до Надавача або ВПР заявник з метою проведення ідентифікації надає адміністратору реєстрації Надавача або ВПР оригінал (для ознайомлення) паспорта громадянина України або іншого документа, що посвідчує особу, відповідно до закону України "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус", та інші документи в паперовій або електронній формі, необхідні для формування кваліфікованих сертифікатів відкритих ключів, визначені переліком, що розміщений на офіційному веб-сайті Надавача.

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

Під час формування кваліфікованих сертифікатів працівників юридичної особи або фізичної особи - підприємця документи, необхідні для формування та видачі кваліфікованого сертифіката відкритого ключа працівнику, підписує уповноважений представник юридичної особи або фізичної особи – підприємця. При цьому Надавач здійснює ідентифікацію працівника, а також ідентифікацію особи уповноваженого представника юридичної особи або фізичної особи - підприємця за паспортом громадянина України або іншим документом, що посвідчує особу, відповідно до закону України "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус", та перевіряє обсяг його повноважень за документом, що визначає повноваження уповноваженого представника юридичної особи або фізичної особи - підприємця, або з використанням інформації, що міститься в ЄДР або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи.

Замість документа, що підтверджує призначення на посаду працівника юридичної особи або фізичної особи – підприємця може бути надане повідомлення про належність працівника до юридичної особи або фізичної особи – підприємця в паперовій або електронній формі, яке підписує особистим підписом або КЕП уповноважений представник юридичної особи або фізичної особи – підприємця.

До розгляду не приймаються документи/копії документів, які мають підчистки, дописки, закреслені слова, інші виправлення або мають пошкодження, внаслідок чого їх текст (фото) неможливо прочитати (розпізнати). Оригінали документів в електронній формі приймаються до розгляду лише за умови чинності накладеного на них удосконаленого або кваліфікованого електронного підпису.

Для підтвердження належного проведення процедури встановлення заявника Надавач забезпечує зберігання електронних копій заяв на формування та документів, які надавались заявниками під час ідентифікації. Створення електронних копій паперових документів виконується адміністратором реєстрації шляхом сканування або фотографування документів. Електронна копія засвідчується кваліфікованим електронним підписом адміністратора реєстрації. Після створення електронних копій паперові документи повертаються заявнику.

Якщо документ надається для перевірки через мобільний застосунок "Дія", електронна копія такого документа надається за допомогою механізму шерингу копій цифрових документів застосунку "Дія".

Електронні копії паперових документів (сканкопії/фотокопії) та оригінали електронних документів, надані під час ідентифікації заявника, зберігаються в електронному вигляді централізовано в БД ПТК Надавача з урахуванням вимог законодавства у сфері захисту інформації та захисту персональних даних.

Під час встановлення особи заявника Надавач може використовувати засоби фотофіксації або відеофіксації факту пред'явлення заявником документів, що посвідчують особу. Збереження фотодокументів та відеозаписів в ІКС Надавача здійснюється після їх засвідчення шляхом створення кваліфікованого електронного підпису адміністратора реєстрації з дотриманням вимог законодавства щодо захисту персональних даних.

3.2.2.2. Порядок віддаленої ідентифікації та автентифікації з використанням мобільного застосунку "Дія"

Віддалена ідентифікація та автентифікація заявника з використанням мобільного застосунку "Дія" відбувається за допомогою засобів ПТК Надавача, інтегрованих у веб-сторінку офіційного веб-сайту Надавача.

Ідентифікація та автентифікація заявника відбувається на підставі ідентифікаційних документів та даних про фізичну особу, що доступні в мобільному застосунку "Дія". При цьому заявник використовує механізм шерингу цифрових копій документів для надання копій документів, що були використані під час ідентифікації. Такі копії документів засвідчуються кваліфікованим електронним підписом власника документів (з використанням сервісу Дія Підпис) та кваліфікованою електронною печаткою державного підприємства "Дія".

У випадку, якщо заявник є уповноваженим представником юридичної особи або фізичної особи - підприємця, додатково здійснюється перевірка інформації про юридичну особу або фізичну особу - підприємця та повноважень її представника за даними ЄДР.

У випадку формування кваліфікованих сертифікатів працівників юридичної особи або фізичної особи - підприємця документи, необхідні для формування та видачі кваліфікованого сертифіката відкритого ключа працівнику, підписує уповноважений представник юридичної особи або фізичної особи – підприємця своїм власним КЕП. При цьому Надавач здійснює ідентифікацію особи уповноваженого представника юридичної особи або фізичної особи - підприємця за його чинним сертифікатом КЕП та перевіряє обсяг його повноважень з використанням інформації, що міститься в ЄДР.

З метою підтвердження належності працівника до юридичної особи або фізичної особи – підприємця Надавачу подається повідомлення про належність працівника до юридичної особи або фізичної особи – підприємця в електронній формі, яке підписує власним КЕП уповноважений представник юридичної особи або фізичної особи – підприємця.

3.2.2.3. Порядок ідентифікації та автентифікації з використанням чинного кваліфікованого сертифіката

У випадку подання заяви на формування сертифіката, що засвідчена кваліфікованим електронним підписом або удосконаленим електронним підписом, що базується на кваліфікованому сертифікаті електронного підпису, користувач шляхом підписання електронної заяви засвідчує, що його реєстраційні дані залишаються незмінними.

Перевірка ідентифікаційних даних заявника, який звертається з заявою в електронній формі, а також законності такого звернення, здійснюється шляхом автентифікації підписувача за результатами перевірки кваліфікованого електронного підпису або удосконаленого електронного підпису, що базується на кваліфікованому сертифікаті електронного підпису, на заяві та встановлення чинності на момент подання заяви кваліфікованого сертифіката відкритого ключа, що містить ідентифікаційні дані особи.

3.2.3. Неперевірена інформація про користувача

Неперевірена інформація про користувача не допускається.

Ідентифікація особи здійснюється Надавачем (відокремленим пунктом реєстрації Надавача) шляхом перевірки та підтвердження належності фізичній чи юридичній особі, яка звернулася за отриманням послуги формування кваліфікованого сертифіката, ідентифікаційних даних особи, отриманих Надавачем (відокремленим пунктом реєстрації Надавача).

3.2.4. Підтвердження повноважень

Під час ідентифікації уповноваженого представника юридичної особи або фізичної особи - підприємця Надавач здійснює автентифікацію такого користувача відповідно до пункту 3.2.2 цих Положень сертифікаційних практик, перевіряє обсяг повноважень за документом, що визначає повноваження уповноваженого представника юридичної особи або фізичної особи - підприємця, чи з використанням інформації, що міститься в ЄДР або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи.

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

3.3. Ідентифікація та автентифікація під час повторного формування сертифіката

Під час повторного формування кваліфікованого сертифіката користувача Надавач повинен перевірити актуальність інформації, що надавалася для попереднього формування кваліфікованого сертифіката.

У разі зміни відомостей, що містяться у кваліфікованому сертифікаті, користувач у триденний строк з дня настання таких змін повідомляє про це Надавача та надає документи, що підтверджують відповідні зміни.

На підставі наданих користувачем документів, що підтверджують зміни відомостей, які містяться у кваліфікованому сертифікаті, Надавач здійснює повторне формування такого сертифіката та його публікацію у разі згоди користувача.

3.4. Ідентифікація та автентифікація користувача під час блокування або скасування сертифіката

Перелік та опис механізмів автентифікації користувачів під час звернень щодо скасування, блокування або поновлення кваліфікованого сертифіката відкритого ключа наведено у Таблиці 3.

Таблиця 3. Перелік та опис механізмів автентифікації користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката.

Тип операції (причина подання заяви)	Форма подання заяви	Механізми підтвердження ідентифікаційних даних
Блокування кваліфікованого сертифіката відкритого ключа	Усна	За ключовою фразою голосової автентифікації, первинний обмін якою між користувачем та Надавачем здійснюється під час подання заяви про формування кваліфікованого сертифіката відкритого ключа
	Письмова паперова	Аналогічні механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які особисто звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, відповідно до п. 3.2.2.1 цих Положень сертифікаційних практик
	Письмова електронна	Аналогічні механізмам віддаленої ідентифікації та автентифікації фізичних осіб та юридичних осіб під час отримання послуги формування кваліфікованого сертифіката відкритого ключа, відповідно до п. 3.2.2.2 цих Положень сертифікаційних практик
	Письмова електронна з КЕП	Аналогічні механізмам підтвердження ідентифікаційних даних користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, відповідно до п. 3.2.2.3 цих Положень сертифікаційних практик
Скасування кваліфікованого сертифіката відкритого ключа	Письмова паперова	Аналогічні механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які особисто звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, відповідно до п. 3.2.2.1 цих Положень сертифікаційних практик
	Письмова електронна	Аналогічні механізмам віддаленої ідентифікації та автентифікації фізичних осіб та юридичних осіб під час отримання послуги формування

		кваліфікованого сертифіката відкритого ключа, відповідно до п. 3.2.2.2 цих Положень сертифікаційних практик
	Письмова електронна з КЕП	Аналогічні механізмам підтвердження ідентифікаційних даних користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, відповідно до п. 3.2.2.3 цих Положень сертифікаційних практик
Поновлення кваліфікованого сертифіката відкритого ключа	Письмова паперова	Аналогічні механізмам підтвердження ідентифікаційних даних фізичних осіб та юридичних осіб, які особисто звернулися за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, відповідно до п. 3.2.2.1 цих Положень сертифікаційних практик
Поновлення кваліфікованого сертифіката відкритого ключа	Письмова електронна	Аналогічні механізмам віддаленої ідентифікації та автентифікації фізичних осіб та юридичних осіб під час отримання послуги формування кваліфікованого сертифіката відкритого ключа, відповідно до п. 3.2.2.2 цих Положень сертифікаційних практик

3.5. Автентифікація при втраті засобу автентифікації

Автентифікація користувача при втраті доступу до особистого ключа здійснюється шляхом надання відповіді на секретне запитання (парольний діалог) або шляхом використання іншої форми автентифікації.

Надавач не використовує номер телефону та адресу електронної пошти користувача як засоби автентифікації користувача для подання заяв про блокування або скасування кваліфікованого сертифіката.

4. ВИМОГИ ДО ЖИТТЄВОГО ЦИКЛУ СЕРТИФІКАТА

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

4.1. Запит на формування сертифіката

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.

Процес реєстрації користувача включає в себе наступні кроки:

- фізичні, юридичні особи, представники юридичних осіб під час отримання кваліфікованих електронних довірчих послуг повинні пройти ідентифікацію особи відповідно до пункту 3.2.2 цих Положень сертифікаційних практик;
- після ідентифікації користувач генерує особистий ключ за допомогою засобів, наданих Надавачем, або надає запити у форматі PKCS#10 на формування кваліфікованого сертифіката, згенеровані ним поза приміщенням Надавача або відокремленим пунктом реєстрації Надавача, для подальшого формування кваліфікованих сертифікатів користувача;
- адміністратор реєстрації Надавача або віддалений адміністратор реєстрації за допомогою спеціалізованого програмного забезпечення формує кваліфікований сертифікат користувача відповідно до наданого запиту на формування кваліфікованого сертифіката.

4.2. Обробка запиту на формування сертифіката

Обробка запиту на формування кваліфікованого сертифіката здійснюється програмними засобами ІКС Надавача за участю адміністратора реєстрації чи віддаленого адміністратора реєстрації, або автоматично за умови забезпечення безперервності процесів генерації пар ключів, формування запитів, передачі їх на обробку захищеними каналами зв'язку, які забезпечують конфіденційність та цілісність даних. Автоматична обробка запитів на формування кваліфікованого сертифіката включає процеси ідентифікації особи користувача та підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката.

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

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

4.3. Формування сертифіката

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

- шляхом надсилання файлу із сформованим кваліфікованим сертифікатом на адресу електронної пошти, вказану користувачем;
- шляхом запису файлу із сформованим кваліфікованим сертифікатом на носій інформації, наданий користувачем;
- шляхом публікації сформованого кваліфікованого сертифіката на веб-сайті Надавача.

4.4. Прийняття сертифіката

Користувач повинен протягом доби перевірити свої ідентифікаційні дані, внесені Надавачем до кваліфікованого сертифіката. Надавач повинен надавати відповідні консультації щодо проведення такої перевірки. Користувач повинен використовувати особистий ключ для створення кваліфікованого електронного підпису тільки після проведення перевірки.

Використання користувачем особистого ключа є фактом визнання ним кваліфікованого сертифіката, що відповідає його відкритому ключу.

У разі виявлення користувачем невідповідності ідентифікаційних даних, внесених Надавачем до кваліфікованого сертифіката, користувач повинен звернутися до Надавача для скасування кваліфікованого сертифіката та формування нового сертифіката.

4.5. Пара ключів та призначення сертифіката

4.5.1. Використання особистого ключа та сертифіката користувачем

Користувач повинен використовувати особистий ключ та кваліфікований сертифікат згідно з вимогами законодавства та відповідно до:

- Політики сертифіката Надавача;
- цих Положень сертифікаційних практик;
- договору про надання кваліфікованих електронних довірчих послуг, укладеного з Надавачем.

Пункт 4.5.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить додаткову інформацію щодо використання особистого ключа та кваліфікованого сертифіката користувачем.

4.5.2. Використання відкритого ключа та сертифіката суб'єктами, які довіряють надавачу

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

- цих Положень сертифікаційних практик;
- Політики сертифіката Надавача.

Пункт 4.5.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить додаткову інформацію щодо використання відкритого ключа та кваліфікованого сертифіката суб'єктами, які довіряють Надавачу.

4.6. Поновлення сертифіката

Надавач не пізніше ніж протягом двох годин поновлює заблокований кваліфікований сертифікат, у разі:

- подання користувачем заяви про поновлення його заблокованого кваліфікованого сертифіката в будь-який спосіб, що забезпечує підтвердження особи користувача (якщо блокування здійснено на підставі заяви про блокування кваліфікованого сертифіката);
- подання заяви про поновлення кваліфікованого сертифіката працівника юридичної особи чи фізичної особи - підприємця за підписом уповноваженої особи відповідної юридичної особи чи фізичної особи - підприємця;

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

– надходження до Надавача повідомлення про прийняття рішення суду про поновлення кваліфікованого сертифіката, що набрало законної сили.

Кваліфікований сертифікат, який був заблокованим, відновлює свою чинність з моменту його поновлення.

Кваліфікований сертифікат вважається поновленим з моменту зміни Надавачем статусу кваліфікованого сертифіката на "поновлений".

4.7. Повторне формування сертифіката

Запит на формування нового кваліфікованого сертифіката для користувачів, які мають чинний кваліфікований сертифікат, подається разом із електронною заявою про формування нового кваліфікованого сертифіката.

Програмні засоби ІКС Надавача із інтегрованими засобами кваліфікованого електронного підпису чи печатки, розміщені на веб-сайті Надавача, забезпечують:

– перевірку чинності попереднього кваліфікованого сертифіката користувача;

– автоматичне формування заяви про формування нового кваліфікованого сертифіката із використанням ідентифікаційних даних, внесених до попереднього кваліфікованого сертифіката користувача;

– створення кваліфікованого електронного підпису чи печатки до цієї заяви із використанням попереднього особистого ключа;

– створення запиту на формування кваліфікованого сертифіката у форматі PKCS#10 на згенеровану нову ключову пару;

– передачу запиту на формування нового кваліфікованого сертифіката разом із заявою про формування нового кваліфікованого сертифіката на обробку до ІКС Надавача.

Створення заяви про формування нового кваліфікованого сертифіката, запиту на формування нового кваліфікованого сертифіката та їх передача на обробку до ІКС Надавача здійснюється із забезпеченням цілісності та конфіденційності інформації за допомогою засобів кваліфікованого електронного підпису чи печатки та засобів КЗІ, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації або державної експертизи таких засобів.

4.8. Зміна сертифіката

Зміна ідентифікаційних даних, що внесені до кваліфікованого сертифіката користувача, є підставою для скасування кваліфікованого сертифіката.

4.9. Блокування та скасування сертифіката

Надавач скасовує сформований ним кваліфікований сертифікат протягом двох годин у разі:

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

- подання заяви про скасування кваліфікованого сертифіката працівника юридичної особи чи фізичної особи - підприємця уповноваженою особою відповідної юридичної особи чи фізичної особи - підприємця;
- надходження до Надавача інформації, що підтверджує:
    - смерть фізичної особи - користувача;
    - державну реєстрацію припинення юридичної особи або припинення підприємницької діяльності фізичної особи - підприємця, що є користувачем;
    - зміну ідентифікаційних даних користувача, які містяться у кваліфікованому сертифікаті;
    - надання користувачем недостовірних ідентифікаційних даних під час формування його кваліфікованого сертифіката;
    - факт компрометації особистого ключа користувача, виявлений користувачем самостійно або контролюючим органом під час здійснення заходів державного контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг;
    - набрання законної сили рішенням суду про скасування кваліфікованого сертифіката, оголошення фізичної особи або фізичної особи - підприємця, що є користувачем, померлою, визнання її безвісно відсутньою, недієздатною, обмеження її цивільної дієздатності, визнання користувача банкрутом.

Надавач блокує сформований ним кваліфікований сертифікат не пізніше ніж протягом двох годин у разі:

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

До переліку суб’єктів, уповноважених подавати запит на скасування (блокування та поновлення) кваліфікованого сертифіката, формування кваліфікованого сертифіката належать фізичні та юридичні особи, які подають до надавача заяви або надають інформацію, що підтверджує підстави для зміни статусу сертифіката, передбачені статтею 25 Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Перелік підстав для зміни статусу кваліфікованого сертифіката на «блокований» та «скасований» із зазначенням суб’єктів подання запитів на зміну статусу та форм підтвердження підстав наведений у Таблиці 4.

Таблиця 4. Перелік підстав для зміни статусу кваліфікованого сертифіката на «блокований» та «скасований»

Підстави для зміни статусу сертифіката	Скасування	Блокування	Підтвердження підстав
Подання користувачем заяви	+	+	Заява користувача
Смерть фізичної особи - користувача	+		Документальне підтвердження
Припинення діяльності користувача (юридичної особи або фізичної особи - підприємця)	+		Документальне або технічне (отримання інформації в електронному вигляді з ЄДР) підтвердження
Зміни ідентифікаційних даних користувача	+		Документальне або технічне (отримання інформації в електронному вигляді з ЄДР) підтвердження
Надання користувачем недостовірних ідентифікаційних даних	+		Документальне підтвердження
Факт компрометації особистого ключа користувача, виявлений самостійно користувачем або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг	+		Документальне підтвердження
Повідомлення користувачем або контролюючим органом про підозру в компрометації особистого ключа користувача електронних довірчих послуг		+	Заява користувача або документальне підтвердження
Набрання законної сили рішенням суду	+	+	Документальне підтвердження
Порушення користувачем істотних умов договору про надання кваліфікованих електронних довірчих послуг		+	Документальне підтвердження

Користувач має право за власним бажанням здійснити блокування кваліфікованого сертифіката. Під блокуванням кваліфікованого сертифіката розуміється тимчасове призупинення чинності кваліфікованого сертифіката.

Після блокування кваліфікованого сертифіката, користувач може поновити чинність кваліфікованого сертифіката.

Заява про скасування, блокування, кваліфікованого сертифіката подається до Надавача у спосіб, що забезпечує підтвердження особи користувача.

Перелік та опис механізмів автентифікації користувачів з питань блокування або скасування кваліфікованого сертифіката наведено у Таблиці 3 цих Положень сертифікаційних практик.

Надавач здійснює цілодобовий прийом та обробку заяв підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів в електронній формі. Прийом та обробка заяв, наданих з використанням інших інформаційних каналів, здійснюється згідно графіку роботи Надавача, розміщеному на офіційному сайті Надавача.

Кваліфіковані сертифікати відкритих ключів скасовуються, блокуються та поновлюються Надавачем не пізніше ніж протягом двох годин від моменту отримання підтвердження підстав для зміни статусу сертифіката і здійснення відповідної перевірки достовірності документальних повідомлень та автентифікації заявників.

4.10. Послуга перевірки статусу сертифіката

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

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

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 пункті 6.4 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

5.1. Контроль фізичної безпеки

Пункт 5.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо вимог до приміщень Надавача та забезпечення фізичного доступу до них.

5.2. Процедурний контроль

Пункт 5.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить

інформацію щодо довірених ролей персоналу Надавача (керівник, адміністратор реєстрації, адміністратор сертифікації, адміністратор безпеки, системний адміністратор, аудитор системи) та їх функціональних обов'язків, щодо кількості осіб, необхідних для виконання завдань, а також довірених ролей персоналу Надавача, що вимагають розподілу обов’язків.

5.3. Контроль персоналу

Пункт 5.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо вимог до кваліфікації, досвіду та допуску персоналу Надавача, вимог та процедур навчання, санкцій за несанкціоновані дії, контролю відокремлених пунктів реєстрації Надавача, документації, яка надається персоналу Надавача.

5.4. Ведення журналу аудиту подій

Пункт 5.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо типів записаних подій, частоти обробки журналу аудиту подій, строків зберігання журналу аудиту подій, захисту журналу аудиту подій, процедур резервного копіювання журналу аудиту подій та питань синхронізації часу.

5.5. Архів документів

Пункт 5.5 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо видів документів та даних, що підлягають архівному зберіганню, строків зберігання архіву та захисту архіву.

5.6. Зміна ключа

Пункт 5.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо підстав та періодичності зміни пари ключів Надавача, порядку використання та доступу до актуального відкритого ключа Надавача.

5.7. Компрометація і аварійне відновлення

Пункт 5.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо процедур обробки інцидентів і компрометації, процедур відновлення, якщо обчислювальні ресурси, програмне забезпечення та/або дані пошкоджені, процедур відновлення після компрометації особистого ключа, можливостей безперервності бізнесу після катастрофи.

5.8. Припинення діяльності надавача

Пункт 5.8 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо підстав припинення діяльності Надавача, порядку надання повідомлення про припинення діяльності, визначення дати припинення діяльності, питань правонаступництва та

передачі документованої інформації, а також Плану припинення діяльності з надання кваліфікованих електронних довірчих послуг.

6. ТЕХНІЧНІ ЗАХОДИ БЕЗПЕКИ

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

6.1. Генерація та встановлення пари ключів

Пункт 6.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо генерації пари ключів Надавача та користувачів, доставки особистого та відкритого ключів користувачам, доставки відкритого ключа Надавача суб’єктам, які довіряють Надавачу, щодо розмірів ключів та основних цілей використання особистих ключів.

6.2. Захист особистого ключа та інженерний контроль криптографічного модуля

Пункт 6.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо керування криптографічним модулем, резервного копіювання особистого ключа, архівації особистого ключа, відновлення особистого ключа, зберігання особистого ключа в криптографічному модулі, активації особистих ключів, деактивації особистих ключів, знищення особистих ключів, можливостей мережного криптографічного модуля.

6.3. Інші аспекти керування парами ключів

Пункт 6.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо архівації відкритого ключа Надавача, строків дії сертифіката та строків використання пари ключів Надавача.

6.4. Дані активації

Пункт 6.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо захисту даних активації особистого ключа.

6.5. Контроль комп'ютерної безпеки

Пункт 6.5 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо спеціальних технічних вимог до комп’ютерної безпеки, рейтингу комп’ютерної безпеки.

6.6. Контроль безпеки життєвого циклу

Пункт 6.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить

інформацію щодо контролю розробки ІКС Надавача, засобів керування безпекою в ІКС Надавача, контролю безпеки протягом життєвого циклу.

6.7. Контроль безпеки мережі

Пункт 6.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо елементів керування безпекою мережі.

6.8. Електронні позначки часу

Пункт 6.8 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо формування та перевірки кваліфікованої електронної позначки часу, наслідків недійсності кваліфікованої електронної позначки часу та процедури отримання Надавачем кваліфікованої електронної позначки часу.

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

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

7.1. Профілі сертифікатів

Пункт 7.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо відомостей, які повинні міститися в кваліфікованих сертифікатах.

7.2. Профілі списку відкликаних сертифікатів

Пункт 7.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо відомостей, які повинні міститися в списках відкликаних сертифікатів.

7.3. Профілі протоколу визначення статусу сертифіката

Пункт 7.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо можливості перевірки статусу кваліфікованого сертифіката користувача в режимі реального часу через електронні комунікаційні мережі загального користування із використанням протоколу OCSP.

8. АУДИТ ВІДПОВІДНОСТІ ТА ІНШІ ОЦІНКИ

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

8.1. Частота або обставини оцінювання

Пункт 8.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо частоти та обставин оцінювання Надавача.

8.2. Особа/кваліфікація оцінювача

Пункт 8.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо вимог до кваліфікації посадових осіб контролюючого органу (КО) та органу з оцінки відповідності (ООВ).

8.3. Відносини експерта з об’єктом оцінки

Пункт 8.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо відносин посадових осіб контролюючого органу (КО) та експертів (аудиторів) органу з оцінки відповідності з об'єктом оцінки (Надавач).

8.4. Теми, охоплені оцінюванням

Пункт 8.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо питань, які підлягають перевірці під час державного контролю та під час оцінки відповідності.

8.5. Дії, вжиті внаслідок порушення

Пункт 8.5 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо дій, які вживаються внаслідок порушення, виявленого за результатами державного контролю або за результатами оцінки відповідності.

8.6. Повідомлення результатів

Пункт 8.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо оформлення результатів державного контролю або оцінки відповідності, надання припису про усунення порушень, виявлених під час державного контролю.

8.7. Самоперевірки

Пункт 8.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо проведення Надавачем регулярних внутрішніх аудитів дотримання встановлених вимог.

9. ІНШІ КОМЕРЦІЙНІ ТА ЮРИДИЧНІ ПИТАННЯ

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

9.1. Ціни і тарифи

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 Надавача, опублікованими на 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 користувача відсутня.

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

Плата за блокування та скасування кваліфікованого сертифіката користувача або доступ до інформації про статус кваліфікованого сертифіката користувача 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;
- зберігання особистих ключів в хмарному сховищі Надавача.

9.1.5. Політика відшкодування

Надавач не відшкодовує сплачені рахунки, послуги по яким надані.

9.2. Фінансова відповідальність

Пункт 9.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо фінансової відповідальності Надавача.

9.3. Конфіденційність ділових даних

Пункт 9.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо змісту та обсягу конфіденційної інформації, що знаходиться в розпорядженні Надавача, а також відповідальності за захист конфіденційної інформації.

9.4. Захист персональних даних

Пункт 9.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо концепції захисту персональних даних, визначення персональних даних, а також персональних даних, що не вважаються конфіденційними, щодо відповідальності за захист персональних даних, щодо згоди на використання персональних даних та обставин розкриття персональних даних.

9.5. Права інтелектуальної власності

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

9.6. Заяви та гарантії

Пункт 9.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо зобов'язань та гарантій Надавача, відокремлених пунктів реєстрації Надавача, користувачів, довіряючих сторін, а також інших учасників.

9.7. Відмова від відповідальності

Пункт 9.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо відмови від гарантій.

9.8. Обмеження відповідальності

Пункт 9.8 Політики сертифіката кваліфікованого надавача електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна» (додаток 1 до цього Регламенту) містить інформацію щодо обставин для обмеження відповідальності Надавача.

9.9. Збитки

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

Ці Положення сертифікаційних практик застосовуються з моменту їх публікації та діють до закінчення строку дії останнього сертифіката, виданого відповідно до цих положень сертифікаційних практик або до моменту припинення діяльності Надавача.

9.11. Індивідуальні комунікації та угоди з суб'єктами інфраструктури відкритих ключів

Надавач здійснює комунікацію з учасниками інфраструктури відкритих ключів шляхом:

– розміщення повідомлень та оголошень на 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 та смс-інформування на номер телефону користувача.

9.12. Зміни

Внесення змін та доповнень до цих Положень сертифікаційних практик здійснюється Надавачем у разі:

– змін вимог, процесів та процедур, описаних у цих Положеннях сертифікаційних практик;
– змін в законодавстві;
– змін у вимогах до надавачів щодо надання послуг.

Нові версії цих Положень сертифікаційних практик після внесення змін до них публікуються на веб-сайті Надавача.

9.13. Положення щодо вирішення спорів

У випадку виникнення спорів або розбіжностей Надавач (ТОВ «Центр сертифікації ключів «Україна») вирішує їх шляхом переговорів та консультацій з учасниками інфраструктури відкритих ключів.

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

9.14. Застосовне право

На відносини, що регулюються цими Положеннями сертифікаційних практик, поширюється чинне законодавство України.

9.15. Дотримання чинного законодавства

Пункт 9.15 Політики сертифіката Надавача містить інформацію щодо нормативно-правових актів, які встановлюють вимоги до надання Надавачем кваліфікованих електронних довірчих послуг.