ЗАТВЕРДЖУЮ
Генеральний директор
державного підприємства «ДІЯ»

_____Дмитро ПЕТРУЩЕНКО
« ____ » _____ 2024 р.

РЕГЛАМЕНТ РОБОТИ

КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ «Дія»

На 196 аркушах

Київ 2024 р.

ЗМІСТ

ВСТУП

Перелік скорочень

ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань
ЄДДР	Єдиний державний демографічний реєстр
ІКС	Інформаційно-комунікаційна система
КЗІ	Криптографічний захист інформації
ЗКЕП	Засіб кваліфікованого електронного підпису чи печатки
ОС	Операційна система
ПЗ	Програмне забезпечення
РНОКПП	Реєстраційний номер облікової картки платника податків
УНЗР	Унікальний номер запису в ЄДДР
ЦОД	Центр обробки даних
CMP	Certificate Management Protocol
OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol
СУІБ	Система управління інформаційною безпекою відповідно до положень стандарту ISO/IEC 27001:2022

Терміни та визначення

В цьому Регламенті терміни та визначення застосовуються у значеннях, наведених у Цивільному кодексі України, Законі України "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”, постанови Кабінету Міністрів України від 5 вересня 2023 р. № 970 «Деякі питання діяльності електронних резидентів (е-резидентів) та ведення інформаційної системи “Е-резидент”», постанові Кабінету Міністрів України від 4 грудня 2019 р. №1137 «Питання Єдиного державного веб порталу електронних послуг та Реєстру адміністративних послуг» та інших нормативно-правових актах з питань криптографічного та технічного захисту інформації.

Статус Регламенту

Цей Регламент є документом кваліфікованого надавача електронних довірчих послуг «Дія» (далі - КНЕДП "Дія"), що визначає організаційно-методологічні, технічні та технологічні умови діяльності КНЕДП "Дія" під час надання кваліфікованих електронних довірчих послуг, включаючи політику сертифіката та положення сертифікаційних практик.

Цей Регламент розроблений відповідно до:

- Закону України “Про електронну ідентифікацію та електронні довірчі послуги” (далі - Закон);

- Закону України “Про електронні документи та електронний документообіг” (зі змінами);
- Закону України “Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань”;
- постанови Кабінету Міністрів України від 28.06.2024 2024 р. № 764 “Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг”;
- постанови КМУ 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”;
- постанова КМУ від 10.10.2018 №821 Про затвердження “Порядку зберігання документованої інформації та її передавання центральному засвідчувальному органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг”;
- постанови Кабінету Міністрів України від 4 грудня 2019 р. №1137 “Питання Єдиного державного веб порталу електронних послуг та Реєстру адміністративних послуг”;
- постанови Кабінету Міністрів України від 5 вересня 2023 р. № 970 “Деякі питання діяльності електронних резидентів (е-резидентів) та ведення інформаційної системи “Е-резидент”;
- інших нормативно-правових актів у сфері надання електронних довірчих послуг.

Положення цього Регламенту поширюються на:

- працівників головного офісу КНЕДП "Дія";
- працівників відокремлених пунктів реєстрації КНЕДП "Дія";
- заявників;
- підписувачів;
- створювачів електронної печатки.

Вимоги цього Регламенту є обов’язковими до виконання працівниками головного офісу та відокремлених пунктів реєстрації КНЕДП "Дія".

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

Вимоги цього Регламенту засновані на принципах дотримання прав та виконання обов’язків суб’єктами надання та отримання кваліфікованих електронних довірчих послуг, які наведено в Законі України «Про електронну ідентифікацію та електронні довірчі послуги».

Будь-яка зацікавлена особа може ознайомитися з положеннями цього Регламенту на офіційному вебсайті КНЕДП "Дія".

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим Регламентом, застосовуються правила міжнародного договору.

Внесення змін та доповнень до Регламенту

Погодження, внесення змін та доповнень до цього Регламенту здійснюється КНЕДП "Дія" відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Про внесення змін та доповнень до цього Регламенту КНЕДП "Дія" повідомляє заявників, підписувачів, створювачів електронних печаток та інших зацікавлених осіб шляхом розміщення зазначених змін та доповнень на офіційному вебсайті КНЕДП "Дія".

Всі зміни та доповнення, внесені КНЕДП "Дія" до цього Регламенту, що не пов'язані зі зміною законодавства, набувають чинності через 10 (десять) календарних днів з дня розміщення зазначених змін і доповнень на офіційному вебсайті КНЕДП "Дія".

Всі зміни та доповнення, внесені КНЕДП "Дія" 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 вебсайті КНЕДП "Дія".

1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО НАДАВАЧА

Повні найменування юридичної особи КНЕДП "Дія": державне підприємство «ДІЯ», State enterprise «DIIA».

Скорочені найменування юридичної особи: ДП «ДІЯ», SE «DIIA».

Повні найменування КНЕДП "Дія": Кваліфікований Надавач електронних довірчих послуг «Дія», Qualified Trust Services Provider «DIIA».

Скорочені найменування КНЕДП "Дія": КНЕДП «Дія», QTSP «DIIA».

Юридична адреса КНЕДП "Дія": 03150, м.Київ, вул. Ділова, буд. 24.

Поштова адреса головного офісу КНЕДП "Дія": 03150, м.Київ, вул. Ділова, буд. 24.

Адреса розміщення головного офісу КНЕДП "Дія": 04070, м. Київ, вул. Василя Тютюнника, буд. 5В.

Телефон: +38 067 107-20-41.

Код згідно з ЄДРПОУ: 43395033.

Електронні адреси офіційних вебсайтів КНЕДП "Дія": ca.diia.gov.ua, ca.informjust.ua.

Адреси електронної пошти головного офісу КНЕДП "Дія": ca@diia.gov.ua, keys@diia.gov.ua, ca@informjust.ua.

Головний офіс КНЕДП "Дія" представлений окремим підрозділом або позаштатною структурою державного підприємства «ДІЯ» (далі – ДП «ДІЯ»), що здійснює організацію надання кваліфікованих електронних довірчих послуг представництвами КНЕДП "Дія" та забезпечує виконання вимог законодавства до кваліфікованих надавачів електронних довірчих послуг.

Представництвами КНЕДП "Дія" є відокремлені пункти реєстрації, що представлені окремими підрозділами або позаштатними одиницями ДП «ДІЯ», або юридичні чи фізичні особи, які на підставі договору з ДП «ДІЯ», здійснюють реєстрацію користувачів засобів електронної ідентифікації чи підписувачів з дотриманням вимог законодавства у сферах електронної ідентифікації, електронних довірчих послуг та захисту інформації.

Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені ДП «ДІЯ» або від імені представництва.

2. ПЕРЕЛІК КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

КНЕДП "Дія" 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 КНЕДП "Дія", посадові обов’язки якого безпосередньо пов’язані з наданням кваліфікованих електронних довірчих послуг у головному офісі КНЕДП "Дія", є працівники, на яких покладено функціональні обов’язки:

- керівника КНЕДП "Дія";
- адміністратора реєстрації;
- адміністратора сертифікації;
- адміністратора безпеки;
- аудитор системи;
- системного адміністратора.

Детальний опис обов’язків персоналу КНЕДП "Дія" визначено в пункті 5.3.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

Детальний опис обов’язків посадових осіб відокремлених пунктів реєстрації КНЕДП "Дія" визначено в пункті 5.3.5. Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (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 “Дія” (додаток 1 до цього Регламенту).

4.1.3 Перелік інформації, що розміщується Надавачем на офіційному вебсайті

В пункті 2.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) наведено перелік інформації, доступ до якої забезпечує КНЕДП "Дія" через офіційний вебсайт.

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 “Дія” (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 “Дія” (додаток 1 до цього Регламенту).

4.1.6 Умови встановлення заявника

Умови встановлення заявника (автентифікації особи) визначено в пункті 3.2.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту), пункті 3.2.2 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) та пункті 3.2.2 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів віддаленого кваліфікованого електронного підпису “Дія.Підпис” (додаток 3 до цього Регламенту).

Умови повноважень уповноваженого представника юридичної особи визначено в пункті 3.2.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту), пункті 3.2.4 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) та пункті 3.2.4 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів віддаленого кваліфікованого електронного підпису “Дія.Підпис” (додаток 3 до цього Регламенту).

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

Механізм автентифікації користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований КНЕДП "Дія" визначено в пункті 3.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) та пункті 3.3 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту).

4.1.8 Механізми автентифікації користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа

Механізм автентифікації користувачів з питань блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа визначено в пункті 3.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) та пункті 3.4 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту).

4.1.9 Опис фізичного середовища

Цей розділ Регламенту містить конфіденційну інформацію про КНЕДП "Дія" відповідно до Положення щодо конфіденційності та класифікації інформації в ДП «ДІЯ», затвердженого наказом ДП “ДІЯ” від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 19 грудня 2023 року № 2".

Процедура доступу до спеціальних приміщень КНЕДП "Дія" визначена в пункті 5.1.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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 КНЕДП "Дія", що може здійснювати перегляд журналів аудиту подій визначено в пункті 5.4 Політика сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

Крім того, фіксуються також події, частота їх перегляду, форма ведення, строк зберігання та персонал КНЕДП "Дія", який має доступ до перегляду цих записів, зазначені в Таблиці 6.

Таблиця 6

Тип події	Частота перегляду	Строк зберігання	Форма ведення	Метод захисту	Доступ на перегляд
Встановлення параметрів (налаштувань) операційних систем та програмного забезпечення	≤ 1 раз на тиждень	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС КНЕДП "Дія"/ зберігання у сховищах (сейфах)	Адміністратор безпеки
Встановлення прав доступу та інших параметрів безпеки	≤ 1 раз на тиждень	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС КНЕДП "Дія"/ зберігання у сховищах (сейфах)	Адміністратор безпеки
Генерація, використання та знищення ключових даних	за необхідності	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС КНЕДП "Дія"/ зберігання у сховищах (сейфах)	Адміністратор безпеки
Внесення, модифікація та видалення реєстраційних даних підписувачів	≤ 1 раз на добу	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС КНЕДП "Дія"/ зберігання у	Адміністратор безпеки

Тип події	Частота перегляду	Строк зберігання	Форма ведення	Метод захисту	Доступ на перегляд
				сховищах (сейфах)	
Формування, блокування, скасування та поновлення сертифікатів ключів, а також формування списків відкликаних сертифікатів	≤ 1 раз на добу	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС КНЕДП "Дія"/ зберігання у сховищах (сейфах)	Адміністратор безпеки
Створення резервних копій та відновлення реєстру сертифікатів та списків відкликаних сертифікатів та іншої важливої інформації	≤ 1 раз на добу	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС КНЕДП "Дія"/ зберігання у сховищах (сейфах)	Адміністратор безпеки
Отримання персоналом доступу до автоматизованої системи КНЕДП "Дія" та її складових частин (вхід до операційної систему тощо)	≤ 1 раз на тиждень	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС КНЕДП "Дія"/ зберігання у сховищах (сейфах)	Адміністратор безпеки
Спроби несанкціонованого доступу до автоматизованої системи КНЕДП	≤ 1 раз на добу	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС КНЕДП "Дія"/	Адміністратор безпеки

Тип події	Частота перегляду	Строк зберігання	Форма ведення	Метод захисту	Доступ на перегляд
"Дія" та її складових частин				зберігання у сховищах (сейфах)	
Збої у роботі автоматизованої системи Надавача та її складових частин	≤ 1 раз на добу	Постійно	Електронна	засобами ОС/ засобами ПЗ ІКС КНЕДП "Дія"/ зберігання у сховищах (сейфах)	Адміністратор безпеки

4.1.12 Порядок ведення архівів Надавача

Види документів та даних, що підлягають архівуванню, строки зберігання архівів, механізм та порядок зберігання і захисту архівів та приміщень, автоматичне резервне копіювання даних, періодичність створення резервних копій та правила збереження з'ємних носіїв визначені в пункті 5.5 Політики сертифікатів кваліфікованого надавача електронних довірчих послуг "Дія" (додаток 1 до цього Регламенту).

Архівні копії журналів аудиту подій мають зберігатися не менше 10-ти 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

Цей розділ Регламенту не входить до обсягу положень, визначених КНЕДП "Дія" для ознайомлення користувачами, та містить конфіденційну інформацію про КНЕДП "Дія" відповідно до Положення щодо конфіденційності та класифікації інформації в ДП «ДІЯ», затвердженого наказом ДП "ДІЯ" від 20.12.2023 № 20231220-3, та викладено в Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами, крім положень, що стосується опису процесу, порядку та умов генерації пар ключів користувачів.

4.1.13.1 Генерація та резервне копіювання особистого ключа Надавача

Процедура генерації та резервного копіювання особистого ключа КНЕДП "Дія" визначена в пункті 6.1.1.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг "Дія" (додаток 1 до цього Регламенту).

Процедура резервного копіювання особистого ключа КНЕДП "Дія" (OCSP, TSP, CMP) викладена в п.6.2.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

4.1.13.2 Генерація та резервне копіювання особистих ключів серверів ІКС Надавача (OCSP, TSP, CMP)

Процедура генерації особистих ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) визначена в пункті 6.1.1.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

Процедура резервного копіювання особистих ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) викладена в п.6.2.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

4.1.13.3 Генерація особистих ключів адміністраторів

Генерація особистих ключів адміністраторів виконується особисто адміністраторами на їх робочих станціях у службових приміщеннях КНЕДП "Дія" відповідно до Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами.

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

Факти генерації особистих ключів адміністраторів заносяться до електронного журналу обліку ключових даних.

Генерація особистого ключа віддаленого адміністратора реєстрації може здійснюватися на робочій станції віддаленого адміністратора реєстрації безпосередньо у приміщеннях відокремленого пункту реєстрації. В цьому випадку генерація ключів здійснюється віддаленим адміністратором реєстрації самостійно, а запит на формування сертифіката віддаленого адміністратора реєстрації передається до центрального офісу КНЕДП "Дія" адміністратору безпеки засобами електронної пошти чи на носієві інформації.

4.1.13.4 Формування кваліфікованого сертифіката відкритого ключа Надавача

Після генерації особистого ключа КНЕДП "Дія" здійснюється формування запиту на кваліфікований сертифікат відкритого ключа КНЕДП "Дія". Формування запиту на кваліфікований сертифікат відкритого ключа КНЕДП "Дія" виконується на центральному сервері у службовому приміщенні КНЕДП "Дія" з використанням особистого ключа КНЕДП "Дія" за участю двох осіб – адміністратора безпеки та адміністратора сертифікації.

Після формування запиту на кваліфікований сертифікат відкритого ключа КНЕДП "Дія", 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 КНЕДП "Дія" від центрального засвідчувального органу, такий сертифікат записується на постійний диск та у базу даних центрального сервера ІКС КНЕДП "Дія".

Після отримання від центрального засвідчувального органу, кваліфікований сертифікат відкритого ключа КНЕДП "Дія" публікується на офіційному вебсайті КНЕДП "Дія".

4.1.13.5 Генерація особистих ключів та формування кваліфікованих сертифікатів відкритих ключів серверів ІКС Надавача (OCSP, TSP, CMP)

Процедура генерації особистих ключів КНЕДП "Дія" визначена в пункті 6.1.1.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

Після генерації особистих ключів КНЕДП "Дія” центральний засвідчувальний орган здійснює формування відповідних кваліфікованих сертифікатів відкритих ключів КНЕДП “Дія”.

Після формування КНЕДП “Дія” кваліфікованих сертифікатів відкритих ключів серверів ІКС КНЕДП “Дія” (OCSP та CMP), такі сертифікати публікуються на офіційному вебсайті КНЕДП “Дія”.

Після формування центральним засвідчувальним органом та отримання КНЕДП "Дія” кваліфікованого сертифіката відкритого ключа TSP серверу ІКС КНЕДП "Дія" такий сертифікат публікується на офіційному вебсайті КНЕДП "Дія".

4.1.13.6 Генерація особистих ключів та формування кваліфікованих сертифікатів відкритих ключів адміністраторів

Генерація особистих ключів адміністраторів реєстрації/віддалених адміністраторів реєстрації та формування їх кваліфікованих сертифікатів відкритих ключів здійснюється відповідно до Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами.

Після генерації особистих ключів адміністраторів реєстрації/віддалених адміністраторів здійснюється формування їх кваліфікованих сертифікатів відкритих ключів адміністратором сертифікації. Формування кваліфікованих сертифікатів відкритих ключів адміністраторів реєстрації/віддалених адміністраторів виконується на центральному сервері ІКС КНЕДП "Дія".

Факти формування кваліфікованих сертифікатів відкритих ключів адміністраторів реєстрації/віддалених адміністраторів заносяться до електронного журналу обліку ключових даних.

4.1.13.7 Використання (введення) особистого ключа Надавача

Процедура використання (введення) особистого ключа КНЕДП "Дія" відбувається відповідно до Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами.

4.1.13.8 Використання (введення) особистих ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP)

Процедура використання (введення) особистого ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) відбувається відповідно до Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами.

4.1.13.9 Використання (введення) особистих ключів адміністраторів

Введення особистих ключів адміністраторів виконується особисто адміністраторами у службових приміщеннях КНЕДП "Дія" на відповідних робочих станціях.

Під час введення ключа здійснюється зчитування даних особистого ключа з ЗКЕП. В процесі введення кваліфікований сертифікат відкритого ключа адміністратора, що містить відкритий ключ, зчитується з постійного диска робочої станції адміністратора.

4.1.13.10 Планова зміна ключів Надавача

Процедура планової зміни ключів КНЕДП "Дія" визначена в пункті 5.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

4.1.13.11 Планова зміна ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP)

Процедура планової зміни ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) визначена в пункті 5.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

Крім того, застосовуються такі особливі вимоги:

Планова зміна ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP), а саме: генерація та резервне копіювання особистих ключів, формування кваліфікованих сертифікатів відкритих ключів та введення для використання особистих ключів, виконується відповідно до пунктів 4.1.13.2 цього Регламенту.

Після введення нових особистих ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP), старі особисті ключі знищуються.

Попередні відкриті ключі серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) зберігається у відповідних кваліфікованих сертифікатів відкритих ключів постійно.

4.1.13.12 Планова зміна ключів адміністраторів

Планова зміна особистих ключів адміністраторів виконується до завершення термінів дії особистих ключів адміністраторів.

Планова зміна ключів адміністраторів, а саме: генерація особистих ключів, формування кваліфікованих сертифікатів відкритих ключів та введення для використання особистих ключів, виконується відповідно до пунктів 4.1.13.3, 4.1.13.6 та 4.1.13.9 цього Регламенту.

Після введення нових особистих ключів адміністраторів, попередні кваліфіковані сертифікати відкритих ключів адміністраторів скасовуються адміністратором безпеки, попередні особисті ключі знищуються.

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

4.1.13.13 Позапланова зміна ключів

Процедура позапланової зміни ключів відповідає процедурі, визначеній в пункті 5.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

Порядок дій персоналу КНЕДП "Дія" у разі компрометації або підозри на компрометацію особистих ключів визначено в пункті 5.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

Факт позапланової зміни ключів заносяться до електронного журналу обліку ключових даних.

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

4.1.13.14 Процедура ідентифікації користувачем відокремлених пунктів реєстрації Надавача

Ідентифікація користувачем відокремленого пункту реєстрації КНЕДП “Дія” здійснюється шляхом перевірки на офіційному вебсайті КНЕДП "Дія" інформації про адресу розташування, графік роботи та контакти такого відокремленого пункту реєстрації.

4.1.13.15 Генерація ключів користувачів

Процедура генерації ключів користувачів визначена в пункті 6.1.1.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

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

Процедури отримання користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги визначена в пункті 6.1.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 КНЕДП "Дія" для формування кваліфікованого сертифіката відкритого ключа визначено у пункті 6.1.3 Політики сертифіката

кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

4.1.16 Порядок захисту та доступу до особистого ключа Надавача

4.1.16.1 Порядок обліку та зберігання ключових даних та документів

Всі ЗКЕП мають бути промарковані та поставлені на облік до початку їх використання, про що робиться відповідний запис до журналу обліку ЗКЕП.

Для забезпечення ідентифікації ЗКЕП можуть використовуватися наявні ідентифікаційні дані у маркуванні – заводські, серійні або інвентарні номери. Інвентарні номери ЗКЕП повинні бути зазначені на наліпках, які наклеюються на корпус носія або прикріплюються у вигляді ярликів.

ЗКЕП однозначно ідентифікується за його типом та ідентифікаційними даними. Всі дії (операції) з ЗКЕП повинні реєструватися у журналі обліку. Всі операції з резервними ЗКЕП повинні реєструватися у журналі обліку так само, як і зі звичайними носіями.

Всі операції з ключовими даними повинні реєструватися у журналі обліку ключових даних.

4.1.16.2 Порядок зберігання носіїв ключової інформації

ЗКЕП повинні зберігатися у сейфах (сховищах) у службових приміщеннях КНЕДП "Дія". Кожен ЗКЕП повинен зберігатися у конверті (коробці, тубусі) разом із обліковою карткою – у вигляді ключового документа.

Облікова картка ключового документа заповнюється адміністратором безпеки підписується керівником КНЕДП "Дія". До облікової картки вноситься інформація про ЗКЕП, ключові дані, що зберігаються на ЗКЕП, включаючи пароль доступу до них, а також, за наявності, пароль доступу до ЗКЕП чи інші ідентифікаційні дані, які необхідні для автентифікації у ЗКЕП (наприклад, інформація про електронні ключі автентифікації для криптомодулів тощо).

ЗКЕП з копіями особистого ключа КНЕДП "Дія" та особистих ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) зберігаються у спеціальному приміщенні в запечатаних конвертах чи коробках, які опечатуються печаткою керівника КНЕДП "Дія" чи адміністратора безпеки.

4.1.16.3 Заходи безпеки під час генерації ключових даних

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

Генерація особистих ключів КНЕДП "Дія" та особистих ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) здійснюються у спеціальному приміщенні КНЕДП "Дія".

Генерація особистих ключів посадових осіб КНЕДП "Дія" здійснюється на робочих станціях у службових приміщеннях КНЕДП "Дія".

Під час генерації особистих ключів КНЕДП "Дія" та особистих ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) двері до спеціального приміщення повинні бути зачиненими, а всі дії проводитись або у середині приміщення за допомогою термінала або за допомогою віддаленого термінала на робочій станції адміністратора безпеки.

Особисті ключі, які зберігаються на ЗКЕП, повинні захищатися на паролях, що складаються не менше ніж з 8 символів, які містять великі та малі латинські літери, цифри та символи.

У випадку, якщо для зберігання та використання особистих ключів використовуються мережні криптомодулі, має забезпечуватися взаємна автентифікації криптомодулів та програмних комплексів (складових частин комплексу ІКС КНЕДП "Дія"). Алгоритм (протокол) взаємної автентифікації повинен реалізовуватися відповідними бібліотеками підтримки (програмними компонентами), які є складовою частиною криптомодулів. Інтерфейси бібліотек підтримки криптомодулів повинні відповідати вимогам до технічних засобів, процесів їх створення, використання та функціонування у складі ІКС під час надання кваліфікованих електронних довірчих послуг.

4.1.16.4 Порядок знищення особистих ключів Надавача, серверів ІКС Надавача

Порядок знищення особистих ключів КНЕДП "Дія", серверів ІКС визначено в пункті 6.2.10 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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

Порядок та умови резервного копіювання особистого ключа КНЕДП "Дія", серверів ІКС КНЕДП "Дія" визначено в пункті 6.2.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

Порядок резервного копіювання особистих ключів КНЕДП "Дія", серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) та адміністраторів визначено у порядку їх генерації (пункти 4.1.13.1 та 4.1.13.2 цього Регламенту).

Факти резервного копіювання особистих ключів КНЕДП "Дія" та серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) заносяться до журналу обліку ключових даних.

Факти відновлення особистих ключів КНЕДП "Дія" та серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) з резервних копій або застосування (переходу до використання) резервних ЗКЕП (мережних криптомодулів) з особистими ключами заносяться до журналу обліку ключових даних. За фактом відновлення особистих ключів чи застосування резервних копій ЗКЕП чи мережних криптомодулів складаються акти.

Резервна копія особистого ключа КНЕДП "Дія" може бути застосована з дозволу керівника КНЕДП "Дія" у випадку виходу з ладу мережного криптомодуля, в якому зберігався та використовувався особистий ключ для відновлення ключа у відремонтованому або заміненому мережному криптомодулі.

Резервні копії особистих ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) можуть бути застосовані у випадку виходу з ладу ЗКЕП з особистими ключами серверів чи мережних криптомодулів, в яких вони зберігалися та використовувалися для заміни основного ЗКЕП чи відновленні ключів у відремонтованому або заміненому мережному криптомодулі.

Резервні копії особистих ключів адміністраторів можуть не створюватися. При цьому адміністраторам можуть видаватися резервні ЗКЕП з попередньо згенерованими особистими ключами. Запити на формування кваліфікованих сертифікатів відкритих ключів адміністраторів зберігаються у адміністратора безпеки. У разі компрометації особистого ключа чи виходу з ладу основного ЗКЕП для адміністратора випускається новий кваліфікований сертифікат, адміністратор починає використовувати резервний ЗКЕП.

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 “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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 Положеннях сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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 “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту).

4.2.3 Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа користувача на офіційному вебсайті Надавача

Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа користувача на офіційному вебсайті КНЕДП "Дія" визначено в пункті 2.2.1 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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 “Дія” (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 “Дія” (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.

Умови використання кваліфікованого сертифіката відкритого ключа користувача та його особистого ключа, а також відомості про наслідки їх неправильного використання зазначаються у договорі про надання кваліфікованої електронної довірчої послуги.

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

Порядок подачі запиту на формування кваліфікованого сертифіката відкритого ключа для користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований КНЕДП "Дія", визначено в пункті 4.7 Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту).

4.2.6 Обставини 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 “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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 “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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 “Дія” щодо

кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту).

4.2.7 Строк закінчення дії кваліфікованого сертифіката відкритого ключа користувача

Строк дії кваліфікованих сертифікатів відкритих ключів користувачів визначено в пункті 1.4.1.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 1 до цього Регламенту).

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 такому сертифікаті із точністю до однієї секунди.

Після настання дати та часу закінчення строку дії кваліфікованого сертифіката відкритого ключа користувача такий кваліфікований сертифікат відкритого ключа вважається нечинним.

4.2.8 Організаційні вимоги

Цим Регламентом, а також іншими нормативними документами КНЕДП "Дія" визначаються вимоги до процедур з управління ризиками, персоналом, операційною безпекою, інцидентами, доказами та архівами, поводження з персональними даними користувачів, процедур встановлення заявника, функціонування відокремлених пунктів реєстрації, опису фізичного середовища.

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 КНЕДП "Дія" використовуються засоби кваліфікованого електронного підпису чи печатки, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів.

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

Надання КНЕДП "Дія" 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 вебсайт КНЕДП "Дія".

Засоби кваліфікованого електронного підпису чи печатки у вигляді SIM-карток надаються користувачам КНЕДП "Дія" або оператором мобільного зв’язку, який обслуговує такі засоби, та який виконує функції представництва КНЕДП "Дія" (відокремленого пункту реєстрації).

Генерація особистих ключів у складі пар ключів у засобах кваліфікованого електронного підпису у вигляді SIM-карток здійснюється вбудованими механізмами цих апаратно-програмних засобів. Допомога при генерації ключів у SIM-картці здійснюється адміністратором реєстрації або працівником представництва КНЕДП "Дія" (відокремленого пункту реєстрації), на якого покладено обов’язки з реєстрації користувачів, та який виконує функції адміністратора реєстрації.

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

Порядок надання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження кваліфікованої електронної позначки часу визначено в пункті 6.9 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

6. СХЕМА ЕЛЕКТРОННОЇ ІДЕНТИФІКАЦІЇ

Схеми електронної ідентифікації затверджені постановою Кабінету Міністрів України від 5 грудня 2023 р. N 1276 «Про затвердження переліку схем електронної ідентифікації» та опубліковані на вебсайті Інтегрованої системи електронної ідентифікації відповідно до абзацу 15 розділу 1 статті 71 Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Додаток 1

до Регламенту роботи кваліфікованого надавача електронних довірчих послуг “Дія”

ПОЛІТИКА СЕРТИФІКАТА

КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ “ДІЯ”

Зміст

1.6.1. Визначення термінів

1.6.2. Перелік скорочень

2. Обов'язки щодо публікації та зберігання

2.1. Репозиторій\вебсайт

2.2. Публікація інформації

2.2.1. Публікація сертифікатів користувачів

2.2.2. Публікація сертифікатів надавача

2.2.3. Доступ до сертифікатів користувачів

2.2.4. Строк закінчення дії сертифіката

2.3. Час та періодичність публікації

2.4. Контроль доступу до репозиторію\вебсайт

3. Ідентифікація та автентифікація

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 за заявою на повторне формування кваліфікованих сертифікатів відкритого ключа

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

3.3.2. Ідентифікація та автентифікація користувача на отримання повторного формування 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

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

1. ВСТУП

1.1. Огляд

Ця Політика сертифіката визначає перелік усіх правил, що застосовуються кваліфікованим надавачем електронних довірчих послуг “Дія” (далі - КНЕДП "Дія") 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) КНЕДП "Дія" та користувачів, зокрема, управління їх статусом (блокування, поновлення та скасування).

Дотримання вимог, визначених у цій Політиці сертифіката, є обов'язковим для керівника профільного підрозділу КНЕДП "Дія" та найманих працівників КНЕДП "Дія", посадові обов'язки яких безпосередньо пов'язані з реєстрацією користувачів, формуванням та обслуговуванню їхніх кваліфікованих сертифікатів (далі - персонал), а також фізичних та юридичних осіб, які на підставі договорів укладених з КНЕДП "Дія"” (державним підприємством “ДІЯ”) безпосередньо чи опосередковано пов'язані з реєстрацією користувачів, формуванням та/або обслуговуванням їхніх кваліфікованих сертифікатів, зокрема, відокремлених пунктів реєстрації КНЕДП "Дія".

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 КНЕДП "Дія" цієї Політики сертифіката, визначають:

- Положення сертифікаційних практик КНЕДП "Дія" щодо кваліфікованих сертифікатів електронного підпису та печатки;
- Положення сертифікаційних практик КНЕДП "Дія" щодо кваліфікованих сертифікатів віддаленого кваліфікованого електронного підпису “Дія.Підпис”.

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 “Дія”.

Скорочена назва документа: Політика сертифіката КНЕДП "Дія".

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; ua-pki	2.1.1.1

Ознака політики сертифікації	ср	2

Кваліфіковані сертифікати, сформовані КНЕДП "Дія", містять об'єктний ідентифікатор (OID) цієї Політики сертифіката, який використовується суб’єктами, які довіряють КНЕДП "Дія", для визначення придатності та надійності 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

КНЕДП "Дія" 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).

КНЕДП "Дія" здійснює реєстрацію користувачів самостійно та/або через відокремлені пункти реєстрації КНЕДП "Дія".

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

1.3.1.1. Права Надавача

КНЕДП "Дія" 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 вони будуть застосовувати для надання кваліфікованих електронних довірчих послуг, з переліку стандартів, визначеного Кабінетом Міністрів України.

1.3.1.2. Обов'язки Надавача

КНЕДП "Дія" 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 КНЕДП "Дія";

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 КНЕДП "Дія" 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 КНЕДП "Дія" 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 КНЕДП "Дія" є органами реєстрації, що представлені окремими підрозділами, позаштатними одиницями державного КНЕДП "Дія" або юридичними чи фізичними особами, які на підставі договору з КНЕДП "Дія", здійснюють реєстрацію користувачів.

До працівників відокремлених пунктів реєстрації КНЕДП "Дія", 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 “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

1.3.3. Користувачі

Користувачами є підписувачі та створювачі електронних печаток, щодо яких КНЕДП "Дія" здійснює їх реєстрацію (самостійно або через відокремлені пункти реєстрації КНЕДП "Дія"), 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 КНЕДП "Дія", та використовують кваліфіковані сертифікати користувачів з метою їх автентифікації, зокрема шляхом перевірки та підтвердження електронного підпису чи печатки.

1.3.5. Інші учасники

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

До інших учасників належать також ЦЗО та КО, які є наглядовими органами щодо КНЕДП "Дія".

ЦЗО, зокрема:

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

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 КНЕДП "Дія";

- інформує громадськість у разі отримання від КНЕДП "Дія" 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 КНЕДП "Дія" 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

КНЕДП "Дія" 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 віддаленого кваліфікованого електронного підпису “Дія.Підпис”, що пов'язує відкритий ключ віддаленого кваліфікованого електронного підпису “Дія.Підпис” 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 “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

1.4.1.2. Строк дії кваліфікованих сертифікатів

Кваліфіковані сертифікати КНЕДП "Дія" формуються ЦЗО зі строком дії не більше 5 років.

Строк дії кваліфікованих сертифікатів КНЕДП "Дія" становить:

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

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

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

   • алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

2. особистого ключа КНЕДП "Дія" 5 років з параметрами, що відповідають таким вимогам:

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

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

   • алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

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

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

5. OCSP 1 рік з параметрами, що відповідають таким вимогам:

- 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).

Кваліфіковані сертифікати користувачів формуються КНЕДП "Дія" зі строком дії 1 або 2 роки.

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

Відповідні Положення сертифікаційних практик КНЕДП "Дія" 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 КНЕДП "Дія" 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 державним підприємством “ДІЯ” (далі - ДП “ДІЯ”).

ДП “ДІЯ” є зареєстрованою відповідно до законодавства юридичною особою публічного права - державним комерційним підприємством, яке засноване на державній власності та належить до сфери управління Міністерства цифрової трансформації України.

Головний офіс КНЕДП "Дія" представлений функціональним підрозділом ДП «ДІЯ», що здійснює організацію надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" та відокремленими пунктами реєстрації КНЕДП "Дія" та забезпечує виконання вимог законодавства до кваліфікованих надавачів електронних довірчих послуг (далі - надавачі).

Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені ДП «ДІЯ» або від імені відокремленого пункту реєстрації КНЕДП "Дія".

Реквізити ДП “ДІЯ”:

- Код згідно з Єдиним державним реєстром підприємств та організацій

України (ЄДРПОУ): 43395033.

- Адреса: вул. Ділова, 24, м. Київ, 03150, Україна.
- Контактний телефон: +38 (067) 258 05 20.
- Адреса електронної пошти: inbox@diia.gov.ua.

Реквізити КНЕДП "Дія":

- Адреси вебсайтів: ca.diia.gov.ua.
- Контактний телефон: +38 (067) 107 20 41.
- Адреси електронної пошти: ca@diia.gov.ua; keys@diia.gov.ua; ca@informjust.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 підписуються керівником профільного підрозділу КНЕДП “Дія”, який відповідає за дотримання, визначених у ній правил, та затверджується генеральним директором ДП “ДІЯ”.

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

1.5.2. Внесення змін до Політики сертифіката

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

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
ЄІС МВС	Єдина інформаційна система Міністерства внутрішніх справ України
ІКС	Інформаційно-комунікаційна система
КЗІ	Криптографічний захист інформації
КО	Контролюючий орган (Адміністрація державної служби спеціального зв'язку та захисту інформації України)
ООВ	Орган з оцінки відповідності
ЦЗО	Центральний засвідчувальний орган (Міністерство цифрової трансформації України)
CMP	Certificate Management Protocol
OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol
СУІБ	Система управління інформаційною безпекою відповідно до положень стандарту ISO/IEC 27001:2022

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

КНЕДП "Дія" повинен забезпечувати:

створення та функціонування вебсайту КНЕДП "Дія";

впровадження, підтримання в актуальному стані та публікацію на вебсайті КНЕДП "Дія" 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.

КНЕДП "Дія" також повинен забезпечувати інформування користувачів про умови отримання кваліфікованих електронних довірчих послуг шляхом розміщення відповідної інформації на вебсайті КНЕДП "Дія".

КНЕДП "Дія" через вебсайт КНЕДП "Дія" (https://ca.diia.gov.ua) забезпечує вільний доступ до:

- відомостей про КНЕДП "Дія";
- даних про внесення відомостей про КНЕДП "Дія" до Довірчого списку;
- Політики сертифіката КНЕДП "Дія";
- відповідних Положень сертифікаційних практик КНЕДП "Дія";
- Загальних положень та умов надання кваліфікованих електронних довірчих послуг користувачам КНЕДП "Дія";
- кваліфікованих сертифікатів КНЕДП "Дія";
- переліку кваліфікованих електронних довірчих послуг, які надає КНЕДП "Дія";
- даних про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг КНЕДП "Дія";
- форм документів, на підставі яких надаються кваліфіковані електронні довірчі послуги
- відомостей про відокремлені пункти реєстрації КНЕДП "Дія";
- 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.

Ця Політика сертифіката доступна 24 години на добу 7 днів на тиждень у форматі лише для читання на вебсайті КНЕДП "Дія".

КНЕДП "Дія" 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 вебсайті КНЕДП "Дія".

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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 КНЕДП "Дія" містять додаткову інформацію.

2.2.2. Публікація сертифікатів Надавача

Кваліфіковані сертифікати КНЕДП "Дія" повинні публікуватися на веб-сайті КНЕДП "Дія" одразу після їх отримання від ЦЗО.

Кваліфіковані сертифікати серверів КНЕДП "Дія" публікуються одразу після їх формування КНЕДП "Дія".

КНЕДП "Дія" забезпечує регулярне оновлення інформації та публікацію кваліфікованих сертифікатів, цієї Політики сертифіката, відповідних Положень сертифікаційних практик КНЕДП "Дія", CRL, договорів, законодавчих актів та інших нормативних документів на вебсайті КНЕДП "Дія": https://ca.diia. gov.ua.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

2.2.3. Доступ до сертифікатів користувачів

Кваліфікований сертифікат користувача після його формування КНЕДП "Дія" 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 КНЕДП "Дія" містять додаткову інформацію.

2.2.4. Строк закінчення дії сертифіката

Строк дії кваліфікованих сертифікатів користувачів становить не більше двох років.

Строк дії кваліфікованих сертифікатів КНЕДП "Дія" становить:

1. СМР 5 років з параметрами, що відповідають таким вимогам:

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

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

- алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

2. особистого ключа КНЕДП "Дія" 5 років з параметрами, що відповідають таким вимогам:

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

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

   - алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

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

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

5. OCSP 1 рік з параметрами, що відповідають таким вимогам:
   - 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).

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

2.3. Час та періодичність публікації

Кваліфіковані сертифікати серверів КНЕДП "Дія"” публікуються одразу після їх формування КНЕДП "Дія".

Кваліфіковані сертифікати серверів КНЕДП "Дія" публікуються одразу після їх формування КНЕДП "Дія".

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

Відповідні Положення сертифікаційних практик КНЕДП "Дія" містять додаткову інформацію.

2.4. Контроль доступу до репозиторію/вебсайту

Репозиторій/вебсайт захищений від несанкціонованого доступу та змін. КНЕДП "Дія" забезпечує цілодобове функціонування власного репозиторію/вебсайту.

За захист інформації на репозиторії/вебсайті та базі даних КНЕДП "Дія" відповідає служба захисту інформації, визначена відповідно до рішення керівництва ДП “ДІЯ” та документів щодо системи управління інформаційною безпекою. Доступ до управління репозиторієм/вебсайтом та базою даних КНЕДП "Дія" надано адміністраторам служби захисту інформації КНЕДП "Дія". Захист інформації на вебсайті, в репозиторії та базі даних КНЕДП "Дія" здійснюється відповідно до Положення щодо конфіденційності та класифікації інформації в ДП «ДІЯ», затвердженого наказом ДП «ДІЯ» від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 19 грудня 2023 року № 2".

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)
UniqueIdentifier(UID)	Ідентифікатор користувача, якому належить кваліфікований сертифікат: - для користувачів, що є фізичними особами, для UID використовується РНОКПП або номер паспорта; - для користувачів, що є фізичними особами - підприємцями, для UID використовується РНОКПП; - для користувачів, що є юридичними особами, для UID використовується код згідно з ЄДРПОУ

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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 всі необхідні позначення (реквізити, атрибути), визначені в стандартах щодо профілів сертифікатів відповідно до пункту 7.1, розділу 7 цієї Політики сертифіката.

3.1.3. Анонімність або використання псевдонімів

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

КНЕДП "Дія" 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 в один із таких способів:

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

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

механізмів ідентифікації, зазначених у підпункті 3.2.2 цієї Політики сертифіката, а також відповідних Положень сертифікаційних практик КНЕДП "Дія".

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

Підтвердження володіння користувачем особистим ключем здійснюється без розкриття особистого ключа.

3.2.2. Автентифікація особи

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

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

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

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

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

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

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

Під час перевірки цивільної правоздатності та дієздатності юридичної особи чи фізичної особи - підприємця (з метою формування кваліфікованого сертифіката електронної печатки) КНЕДП "Дія" зобов'язаний використовувати інформацію про юридичну особу чи

фізичну особу - підприємця, що міститься в ЄДР або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи, а також пересвідчитися, що обсяг цивільної правоздатності та дієздатності юридичної особи чи фізичної особи - підприємця є достатнім для формування та видачі кваліфікованого сертифіката.

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

У випадках передачі обслуговування кваліфікованих сертифікатів користувачів та документованої інформації, на підставі якої були сформовані зазначені сертифікати, від надавача, який припиняє свою діяльність, до КНЕДП "Дія" 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 КНЕДП "Дія" містять додаткову інформацію.

3.2.3. Неперевірена інформація про користувача

Неперевірена інформація про користувача не допускається.

Відповідні Положення сертифікаційних практик КНЕДП "Дія" містять додаткову інформацію.

3.2.4. Підтвердження повноважень

Уповноважений представник юридичної особи або фізичної особи - підприємця підписує документи, необхідні для формування та видачі кваліфікованого сертифіката працівнику юридичної особи або фізичної особи - підприємця. КНЕДП "Дія" під час формування та видачі кваліфікованого сертифіката працівнику юридичної особи або фізичної особи - підприємця здійснює ідентифікацію працівника, а також ідентифікацію особи уповноваженого представника юридичної особи або фізичної особи - підприємця здійснює ідентифікацію працівника, 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, чи з використанням інформації, що міститься в ЄДР або в торговельному, банківському чи судовому реєстрі, який ведеться країною резидентства іноземної юридичної особи.

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

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

Відповідні Положення сертифікаційних практик КНЕДП "Дія" містять додаткову інформацію.

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

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

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

Для формування нового кваліфікованого сертифіката користувача, що має чинний кваліфікований сертифікат, сформований КНЕДП "Дія", такий користувач проходить процедуру автентифікації за поданою в електронній формі до КНЕДП "Дія" 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 “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять додаткову інформацію.

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

У разі, якщо кваліфікований сертифікат користувача скасовано, для формування нового кваліфікованого сертифіката в КНЕДП "Дія" 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.

Перевірка ідентифікаційних даних користувача, який звертається із заявою про блокування або скасування кваліфікованого сертифіката в електронній формі, а також законності такого звернення, здійснюється шляхом автентифікації та ідентифікації користувача за допомогою:

- засобів електронної ідентифікації, які належать до схеми електронної ідентифікації КНЕДП "Дія" “DIIA.PKI” та підтвердження повноважень користувача за результатами перевірки кваліфікованого електронного підпису на заяві та встановленням чинності кваліфікованого сертифіката користувача, що містить ідентифікаційні дані особи на момент подання заяви;
- засобів електронної ідентифікації, які належать до схеми електронної ідентифікації КНЕДП "Дія" “DIIA.PKI.Remote” та підтвердження повноважень користувача за результатами перевірки кваліфікованого електронного підпису на заяві та встановленням чинності кваліфікованого сертифіката користувача, що містить ідентифікаційні дані особи на момент подання заяви.

Схеми ідентифікації КНЕДП "Дія" затверджені постановою Кабінету Міністрів України від 5 грудня 2023 р. N 1276 «Про затвердження переліку схем електронної ідентифікації» та опубліковані на веб сайті Інтегрованої системи електронної ідентифікації відповідно до абзацу 15 розділу 1 статті 7^1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Для блокування або скасування кваліфікованого сертифіката користувача, що має чинний кваліфікований сертифікат, сформований КНЕДП "Дія", такий користувач проходить процедуру автентифікації за поданою в електронній формі до КНЕДП "Дія" заявою про блокування або скасування кваліфікованого сертифіката.

Пункт 4.9 цієї Політики сертифіката та відповідних Положень сертифікаційних практик КНЕДП "Дія" 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 “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту) містять 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 КНЕДП "Дія" за участю адміністратора реєстрації, працівника відокремленого пункту реєстрації КНЕДП "Дія", на якого покладено обов’язки з реєстрації користувачів, та який виконує функції адміністратора реєстрації, або автоматично за умови забезпечення безперервності процесів генерації пар ключів, формування запитів, передачі їх на обробку захищеними каналами зв’язку, які забезпечують конфіденційність та цілісність даних. Автоматична обробка запитів не виключає процесів ідентифікації особи користувача та підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката.

Під час обробки запиту на формування кваліфікованого сертифіката засобами ІКС КНЕДП "Дія" 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 у заяві на формування кваліфікованого сертифіката;
- шляхом запису файлу із сформованим кваліфікованим сертифікатом на носій інформації, наданий користувачем;

- шляхом публікації сформованого кваліфікованого сертифіката на веб сайті КНЕДП "Дія".

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 КНЕДП "Дія" за посиланням https://ca.diia.gov.ua/certificates-search відразу після обробки запиту на сертифікат.

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

Перевірка працездатності свого особистого ключа та ідентифікаційних даних внесених до кваліфікованого сертифіката здійснюється користувачем за допомогою зчитування особистого ключа на вебсайті КНЕДП "Дія" у розділі “знайти сертифікат” або за допомогою спеціалізованого програмного забезпечення, що доступне на вебсайті КНЕДП "Дія" https://ca.diia.gov.ua/.

У разі виявлення користувачем протягом однієї доби невідповідності ідентифікаційних даних, внесених КНЕДП "Дія" до кваліфікованого сертифіката, користувач повинен звернутися до КНЕДП "Дія" для скасування кваліфікованого сертифіката та безкоштовного формування нового сертифіката. У разі звернення користувача після 24 годин формування сертифіката здійснюється на платній основі.

У разі невідповідності ідентифікаційних даних, внесених КНЕДП "Дія" до кваліфікованого сертифіката та виявлених КНЕДП "Дія" до моменту надання сформованого кваліфікованого сертифіката користувачу, посадовою особою КНЕДП "Дія" здійснюється переформування кваліфікованого сертифіката із використанням попередньо засвідченого відкритого ключа та з дотриманням вимог щодо недопущення перевищення часу чинності особистого ключа та відповідного йому відкритого ключа більше двох років. Посадова особа, що здійснила переформування кваліфікованого сертифіката, складає акт, в якому зазначається дата та час скасування кваліфікованого сертифіката, ідентифікаційні дані користувача, що містяться в кваліфікованому сертифікаті та невідповідні ідентифікаційні дані користувача, що зазначені у заяві про формування кваліфікованого сертифіката. Акт підписується посадовою особою КНЕДП "Дія", що здійснила переформування кваліфікованого сертифіката, та долучається до документів (засвідчених в установленому порядку копій документів), що використовувалися під час встановлення особи та реєстрації користувача.

4.5. Використання пари ключів і сертифіката

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

4.5.1. Використання особистого ключа та 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 КНЕДП "Дія" 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 КНЕДП "Дія";

- Загальних положень та умов надання кваліфікованих електронних довірчих послуг користувачам КНЕДП "Дія";

- Договору про надання кваліфікованих електронних довірчих послуг, укладеного з КНЕДП "Дія" (ДП “ДІЯ”).

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

Кваліфіковані сертифікати користувачів, сформовані КНЕДП "Дія", можуть використовуватися будь-якими суб’єктами, які довіряють КНЕДП "Дія", 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 КНЕДП "Дія", 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 КНЕДП "Дія", повинен виконати такі перевірки:

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

- перевірити статус кваліфікованого сертифіката КНЕДП "Дія" під час накладання кваліфікованого електронного підпису чи печатки користувачем.

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

Суб’єкт, який довіряє КНЕДП "Дія", несе відповідальність за те, що не дотримувалась вищевказаної процедури перевірки або виконувала перевірку, знаючи, що кваліфікований сертифікат не чинний на момент перевірки.

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

- цієї Політики сертифіката;

- відповідних Положень сертифікаційних практик КНЕДП "Дія".

4.6. Поновлення сертифіката

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

КНЕДП "Дія" зобов'язаний забезпечувати, зокрема:

- цілодобовий прийом та перевірку заяв в електронній формі користувачів про поновлення їхніх кваліфікованих сертифікатів, які були заблоковані КНЕДП "Дія";

- прийом та перевірку заяв у паперовій формі користувачів про поновлення їхніх кваліфікованих сертифікатів, які були заблоковані КНЕДП "Дія", протягом одного робочого дня після надходження заяви та згідно з режимом роботи КНЕДП "Дія";

- поновлення кваліфікованих сертифікатів, які були заблоковані КНЕДП "Дія", відповідно до вимог Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

Інформування користувачів про закінчення терміну дії його кваліфікованого сертифіката здійснюється КНЕДП "Дія" за 7 днів до закінчення кваліфікованого сертифіката,

шляхом надсилання смс повідомлень на номер телефону користувача, що міститься в заяві про реєстрацію.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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.

КНЕДП "Дія" здійснює формування кваліфікованого сертифіката користувача, в тому числі, на підставі чинного кваліфікованого сертифіката, сформованого КНЕДП "Дія", 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.

Сформувати новий кваліфікований сертифікат користувач також може після закінчення строку дії та у разі нагальної потреби (компрометації особистого ключа чи паролю до нього, втрати особистого ключа, зміни відомостей, що містяться в кваліфікованому сертифікаті користувача), звернувшись в пункт обслуговування КНЕДП "Дія" або відокремлений пункт реєстрації КНЕДП "Дія".

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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 “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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.

КНЕДП "Дія" зобов'язаний забезпечувати, зокрема:

- цілодобовий прийом та перевірку заяв в електронній формі користувачів про скасування та блокування їхніх кваліфікованих сертифікатів, сформованих КНЕДП "Дія";

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

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

Користувач має право за власним бажанням здійснити скасування кваліфікованого сертифіката шляхом проходження електронної ідентифікації за допомогою засобів електронної ідентифікації, які мають високий та середній рівень довіри, відповідно до пункту 3.4 цієї Політики.

Користувач має право за власним бажанням здійснити блокування кваліфікованого сертифіката. Блокування кваліфікованого сертифіката може здійснюватись КНЕДП "Дія" за паперовою заявою про зміну статуса кваліфікованого сертифіката або після ідентифікації користувача за ключовою фразою внесеною до заяви про реєстрацію. Під блокуванням кваліфікованого сертифіката розуміється тимчасове призупинення чинності кваліфікованого сертифіката строком до 30 календарних днів.

Після блокування кваліфікованого сертифіката, користувач може протягом 30 календарних днів поновити чинність кваліфікованого сертифіката. Блокований кваліфікований сертифікат буде автоматично скасований КНЕДП "Дія", якщо протягом зазначеного строку користувач не поновить його чинність.

Кваліфікований сертифікат втрачає чинність з моменту зміни його статусу на "скасований".

Скасований кваліфікований сертифікат поновленню не підлягає.

Кваліфікований сертифікат вважається заблокованим з моменту зміни його статусу на "заблокований".

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

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

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

- у кожному списку відкликаних сертифікатів зазначається граничний строк його дії до видання нового списку;
- новий список відкликаних сертифікатів може бути опубліковано до настання граничного строку його дії до видання наступного списку;

- на список відкликаних сертифікатів повинен бути накладений кваліфікований електронний підпис чи печатка КНЕДП "Дія".

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 сертифікати, які були сформовані КНЕДП "Дія".

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

Відповідні Положення сертифікаційних практик КНЕДП "Дія" містять додаткову інформацію.

4.10. Служби статусу сертифіката

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

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 КНЕДП "Дія" повинні бути розділені на функціональні зони за рівнями безпеки приміщень, встановленими КНЕДП "Дія".

Приміщення КНЕДП "Дія" за рівнями безпеки поділяються на спеціальні та службові. Для кожного рівня безпеки приміщень визначаються 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 КНЕДП "Дія", мають розташовуватися в захищеному та безпечному середовищі з фізичним захистом від вторгнення, контролем доступу через периметр безпеки та сигналізацією для виявлення вторгнення.

Доступ до приміщень КНЕДП "Дія" забезпечено відповідно до документів СУІБ Положення щодо фізичної безпеки в ДП «ДІЯ» DIIA/13 – ISMS – Ph - SOP/1 - Physical and environmental security, затвердженого наказом ДП “ДІЯ” від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 19 грудня 2023 року № 2".

5.1.2. Фізичний доступ

Доступ до спеціальних та службових приміщень КНЕДП "Дія" (безпечна зона) забезпечується із застосуванням організаційно-технічних заходів контролю (фізичний та логічний контроль) відповідно до документів СУІБ, а саме: Положення щодо фізичної безпеки в ДП «ДІЯ» DIIA/13 – ISMS – Ph - SOP/1 - Physical and environmental security, затверджених наказом ДП «ДІЯ» від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від від 19 грудня 2023 року № 2".

Право доступу до спеціальних приміщень центру обробки даних (ЦОД) мають право тільки керівник профільного підрозділу КНЕДП "Дія" та персонал КНЕДП "Дія" відповідно до своїх службових обов’язків, які внесені у відповідний перелік авторизованих співробітників КНЕДП "Дія", що мають доступ до спеціальних приміщень КНЕДП "Дія".

Доступ не авторизованих співробітників до спеціальних приміщень здійснюється:

1) у штатних ситуаціях (планові перевірки, ремонтно-відновлювальні роботи тощо) – за рішенням генерального директора ДП «ДІЯ» або особи, що виконує його обов’язки, на підставі розгляду службової записки, поданої працівником, на якого покладено обов’язки керівника служби захисту інформації ІКС КНЕДП "Дія"”, та з подальшим включенням таких працівників до Заявки на доступ;

2) в екстрених ситуаціях (пожежа, затоплення, стихійне лихо, аварійні випадки тощо) – без дозволу генерального директора ДП «ДІЯ» або особи, що виконує його обов'язки, з обов'язковим внесенням запису про причини екстреного доступу на об'єкт до відповідного розділу Формуляру "Реєстрація надзвичайних подій та відмов ІКС КНЕДП "Дія".

При вході в ЦОД працівник охорони ідентифікує авторизованих співробітників КНЕДП "Дія" за документами, що посвідчують особу (паспорт громадянина України, водійське посвідчення).

Реєстрація доступу до спеціального приміщення здійснюється в електронному або паперовому журналі доступу, що знаходиться в ЦОД.

Серверна шафа в якій розміщено обладнання ІКС КНЕДП "Дія" замикається на ключ та опечатується відповідальними працівниками КНЕДП "Дія".

Територія ЦОД та серверне приміщення де розміщено обладнання ІКС КНЕДП "Дія" обладнано системою відеоспостереження, що функціонує цілодобово, журнали відеоспостереження зберігаються в ЦОД.

Внесення/винесення обладнання із спеціального приміщення здійснюється на підставі акту внесення/винесення обладнання підписаного відповідальними співробітниками.

ІКС КНЕДП "Дія" складається з двох однакових, незалежних один від одного майданчиків (основний та резервний), що розміщені віддалено один від одного на відстані більше 100 км.

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 внутрішньої інструкції ДП "ДІЯ", що є складовою документації СУІБ, зокрема до Процедури проведення попередньої репутаційної перевірки, зокрема перевірки благонадійності кандидата на вакантні посади ДП "ДІЯ" DIIA/13 – ISMS – Ppl - PPL/1 – SOP/1 - Screening, затвердженої наказом ДП "ДІЯ" від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 19 грудня 2023 року № 2".

5.3.1. Довірені ролі персоналу

Персоналом КНЕДП "Дія" є:

- керівник профільного підрозділу КНЕДП "Дія";
- адміністратор реєстрації;

- адміністратор сертифікації;
- адміністратор безпеки;
- аудитор системи;
- системний адміністратор.

5.3.1.1. Керівник

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

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

Керівник профільного підрозділу КНЕДП "Дія" безпосередньо приймає участь та контролює процес генерації та резервного копіювання ключів КНЕДП "Дія" з правами та обов’язками адміністратора сертифікації.

Керівник профільного підрозділу КНЕДП "Дія" представляє КНЕДП "Дія" у випадках, передбачених Політикою сертифіката та Положеннями сертифікаційних практик ЦЗО.

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 КНЕДП "Дія".

До працівників відокремлених пунктів реєстрації КНЕДП "Дія", 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 КНЕДП "Дія", а також створення їх резервних копій.

Основними обов’язками адміністратора сертифікації є:

- участь у генерації пар ключів КНЕДП "Дія" та створенні резервних копій особистих ключів КНЕДП "Дія";
- зберігання особистих ключів КНЕДП "Дія" та їх резервних копій;
- забезпечення використання особистих ключів КНЕДП "Дія" під час формування та обслуговування кваліфікованих сертифікатів КНЕДП "Дія" та користувачів;
- перевірка заяв про формування кваліфікованих сертифікатів КНЕДП "Дія" на відповідність вимогам цієї Політики сертифікації та відповідних Положень сертифікаційних практик;
- участь у знищенні особистих ключів КНЕДП "Дія";
- забезпечення ведення, архівування та відновлення баз даних кваліфікованих сертифікатів користувачів;
- забезпечення публікації кваліфікованих сертифікатів користувачів та списків відкликаних сертифікатів на вебсайті КНЕДП "Дія";
- створення резервних копій кваліфікованих сертифікатів користувачів;

- зберігання кваліфікованих сертифікатів відкритих ключів користувачів, їх резервних копій, списків відкликаних сертифікатів та інших важливих ресурсів ІКС КНЕДП "Дія".

Додатковими обов’язками адміністратора сертифікації є ведення журналів обліку адміністратора сертифікації, передбачених внутрішньою документацією ІКС КНЕДП "Дія".

5.3.1.4. Адміністратор безпеки

Адміністратор безпеки відповідає за належне функціонування ІКС КНЕДП "Дія.

Основними обов’язками адміністратора безпеки є:

- участь у генерації пар ключів КНЕДП "Дія" та створенні резервних копій особистих ключів КНЕДП "Дія";
- контроль за формуванням, обслуговуванням, створенням та перевіркою резервних копій кваліфікованих сертифікатів КНЕДП "Дія", користувачів та списків відкликаних сертифікатів;
- контроль за зберіганням особистих ключів КНЕДП "Дія" та їх резервних копій, особистих ключів адміністраторів;
- участь у знищенні особистих ключів КНЕДП "Дія", контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;
- організація розмежування доступу до ресурсів ІКС КНЕДП "Дія";
- забезпечення спостереження за функціонуванням ІКС КНЕДП "Дія" (реєстрація подій в ІКС КНЕДП "Дія", моніторинг подій тощо);
- забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування ІКС КНЕДП "Дія" після збоїв, відмов;
- забезпечення режиму доступу до приміщень КНЕДП "Дія", в яких розміщена ІКС КНЕДП "Дія";
- ведення журналів обліку адміністратора безпеки, визначених документацією щодо ІКС КНЕДП "Дія" або звітності, що передбачена СУІБ
- проведення перевірок відповідності положень внутрішньої організаційно-розпорядчої документації КНЕДП "Дія" та СУІБ;
- контроль за дотриманням персоналом КНЕДП "Дія" положень внутрішньої організаційно-розпорядчої документації КНЕДП "Дія" та документації СУІБ;
- контроль за веденням баз даних КНЕДП "Дія".

Адміністратор безпеки відповідає за проведення перевірок дотримання персоналом КНЕДП "Дія" та відокремленими пунктами реєстрації КНЕДП "Дія" положень внутрішньої організаційно-розпорядчої документації КНЕДП "Дія" та документації СУІБ, затвердженої

наказами ДП «ДІЯ» від 12.10.2023 № 20231012-2 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 09 жовтня 2023 року № 1", від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 09 жовтня 2023 №2".

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 КНЕДП "Дія".

Основними обов'язками системного адміністратора є:

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

5.3.1.6. Аудитор системи

Аудитор системи відповідає за належне функціонування ІКС КНЕДП "Дія".

Основними обов'язками аудитора системи є:

- проведення перевірок журналів аудиту подій, що реєструють засоби та обладнання програмно-технічного комплексу (далі - технічні засоби) ІКС КНЕДП "Дія";
- контроль за веденням архіву КНЕДП "Дія".

5.3.2. Вимоги щодо кваліфікації, досвіду та допуску персоналу

Персонал КНЕДП "Дія" повинен мати необхідні для надання кваліфікованих електронних довірчих послуг знання, досвід і кваліфікацію та дотримуватись положень та

вимог зазначених в СУІБ Політиці забезпечення інформаційної безпеки у питаннях, пов’язаних з персоналом в ДП «ДІЯ» DIIA/13 – ISMS – Ppl - PPL/1 – Human_resource_security, затвердженій наказом ДП «ДІЯ» від 12.10.2023 № 20231012-2 “Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 09 жовтня 2023 року № 1”.

Адміністратором сертифікації, адміністратором безпеки, системним адміністратором, аудитором системи може бути особа, яка має вищу освіту за спеціальністю у сферах інформаційних технологій, захисту інформації або кібербезпеки, а також стаж роботи за фахом у зазначених сферах не менше трьох років.

5.3.3. Вимоги та процедури навчання персоналу

Керівник профільного підрозділу КНЕДП "Дія" зобов’язаний забезпечити створення умов для безперервної особистої освіти та постійне підвищення кваліфікації персоналу КНЕДП "Дія" у сферах інформаційних технологій, захисту інформації або кібербезпеки та захисту персональних даних.

Персонал КНЕДП "Дія" регулярно бере участь в семінарах, конференціях та зустрічах щодо надання кваліфікованих електронних довірчих послуг, інформаційних технологій, захисту інформації, кібербезпеки та захисту персональних даних. Проходження навчання повинно підтверджуватись дипломом, сертифікатом тощо.

Персонал КНЕДП "Дія" також проходить навчання із здачею тестів відповідно до розділу Навчання вебсайту http://suib.office.diia/is-course.

5.3.4. Санкції за несанкціоновані дії персоналу

Керівником профільного підрозділу КНЕДП "Дія" встановлена чітка система дисциплінарних стягнень за недотримання персоналом КНЕДП "Дія" своїх посадових обов’язків, вимог нормативно-правових актів у сфері електронних довірчих послуг і вимог внутрішньої організаційно-розпорядчої документації КНЕДП "Дія" та Політиці забезпечення інформаційної безпеки у питаннях, пов’язаних з персоналом в ДП «ДІЯ» DIIA/13 – ISMS – Ppl - PPL/1 – Human_resource_security, затвердженої наказом ДП «ДІЯ» від 12.10.2023 № 20231012-2“Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 09 жовтня 2023 року № 1”.

Недотримання персоналом КНЕДП "Дія" своїх посадових обов’язків, вимог нормативно-правових актів у сфері електронних довірчих послуг, вимог внутрішньої організаційно-розпорядчої документації КНЕДП "Дія" та Політиці забезпечення інформаційної безпеки у питаннях, пов’язаних з персоналом в ДП «ДІЯ» DIIA/13 – ISMS – Ppl - PPL/1 – Human_resource_security, затвердженої наказом ДП «ДІЯ» від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 09 жовтня 2023 №2". в межах організації з урахуванням режиму роботи КНЕДП "Дія"

передбачає дисциплінарні стягнення, адміністративну та кримінальну відповідальність, передбачені такими документами:

- Колективним договором державного підприємства «ДІЯ» на 2024-2026 роки;
- договором на здійснення представництва КНЕДП "Дія" (для відокремлених пунктів реєстрації КНЕДП "Дія");
- Кодексом України про адміністративні правопорушення;
- Кримінальним кодексом України.

5.3.5. Контроль відокремлених пунктів реєстрації

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

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

На працівників відокремлених пунктів реєстрації КНЕДП "Дія" покладено такі функціональні обов’язки:

- віддаленого адміністратора реєстрації;
- відповідального за захист інформації на відокремленому пункті реєстрації КНЕДП "Дія".

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

З числа віддалених адміністраторів реєстрації на відокремленому пункті реєстрації КНЕДП "Дія" призначаються відповідальні за захист інформації.

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

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

- організація експлуатації та технічного обслуговування апаратних та програмних засобів відокремленого пункту реєстрації КНЕДП "Дія";
- участь у впровадженні та забезпеченні функціонування ІКС КНЕДП "Дія" відокремленого пункту реєстрації КНЕДП "Дія";
- контроль за роботою програмного комплексу відокремленого пункту реєстрації КНЕДП "Дія";

- контроль за використанням особистих ключів персоналу відокремленого пункту реєстрації КНЕДП "Дія";
- участь у створенні та введенні в експлуатацію ІКС КНЕДП "Дія" відокремленого пункту реєстрації КНЕДП "Дія".

Допускається виконання функцій відповідального за захист інформації на відокремленому пункті реєстрації КНЕДП "Дія" системним адміністратором та адміністратором безпеки у частині, що не суперечить їхнім аналогічними функціями по відношенню до інших складових ІКС КНЕДП "Дія".

5.3.6. Документація, яка надається персоналу

Організаційно-правовий статус керівника профільного підрозділу і персоналу КНЕДП "Дія", 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 КНЕДП "Дія" повинні бути ознайомлені з положеннями їх посадових інструкцій, діяти відповідно до своїх посадових завдань та функцій та з документом СУІБ Політика забезпечення інформаційної безпеки у питаннях, пов'язаних з персоналом в ДП «ДІЯ» DIIA/13 – ISMS – Ppl - PPL/1 – Human_resource_security, затверджена наказом ДП «ДІЯ» від 12.10.2023 № 20231012-2"Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 09 жовтня 2023 року № 1".

Персонал КНЕДП "Дія" повинен бути повідомлений про зміни в організації процесів КНЕДП "Дія", 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 КНЕДП "Дія" тощо;
- заміна технічних засобів ІКС КНЕДП "Дія" та пар ключів;
- формування, блокування, скасування та поновлення сертифікатів, формування списків відкликаних сертифікатів (CRL);
- спроби несанкціонованого доступу до ІКС КНЕДП "Дія"";
- надання доступу персоналу до ІКС КНЕДП "Дія";

- зміни системних конфігурацій та технічне обслуговування ІКС КНЕДП "Дія";
- збої в роботі ІКС КНЕДП "Дія"";
- 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

КНЕДП "Дія" зберігає журнали аудиту подій на місці їх створення протягом 10 років, після чого забезпечує їх передачу на архівне зберігання.

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.

На записи подій у журналах аудиту подій повинен бути накладений кваліфікований електронний підпис адміністратора безпеки.

5.4.5. Процедури резервного копіювання журналу аудиту подій

Резервне копіювання журналу аудиту подій здійснюється КНЕДП "Дія" відповідно до внутрішньої документації із захисту ІКС КНЕДП "Дія" та документа СУІБ Процедури ведення журналу подій на державному підприємстві «ДІЯ» DIIA/13 – ISMS – Tech – GU/2 - SOP/3 -Event logging, затвердженої наказом ДП «ДІЯ» від 12.02.2024 № 20240212-1 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 08 лютого 2024 року № 3".

5.4.6. Синхронізація часу

Синхронізацію часу у технічних засобах ІКС КНЕДП "Дія" на основному та резервному майданчику забезпечує комплекс засобів синхронізації часу з урахуванням документа Процедури синхронізації часу на державному підприємстві «ДІЯ» DIIA/13 – ISMS – Tech – GU/2 - SOP/6 - Clock synchronization, затвердженої наказом ДП «ДІЯ» від 25.03.2024 № 20240325-1 “Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 22 березня 2024 року № 4”.

Комплекс засобів синхронізації часу забезпечує отримання сигналів синхронізації часу з серверів взаємодії ІКС КНЕДП "Дія" (далі - NTP-серверів), резервних NTP-серверів, синхронізованих з державним еталоном одиниць часу і частоти, серверів синхронізації часу GPS КНЕДП «Дія» та синхронізацію системного часу на технічних засобах ІКС КНЕДП "Дія".

Сервери синхронізації часу GPS КНЕДП "Дія" отримують сигнали часу від GPS-приймача, а також резервних джерел синхронізації часу: зовнішніх NTP-серверів ЦЗО (czo.gov.ua, time.czo.gov.ua), ntp.metrology.kharkov.ua та kyivtime.org, що синхронізовані з Державним еталоном одиниць часу і частоти та передають синхронізовані дані до серверів взаємодії КНЕДП "Дія".

Основним джерелом часу для ІКС КНЕДП "Дія" є NTP-сервери.

Всі сервери, обладнання КЗІ та персональні комп'ютери КНЕДП "Дія" підключаються до NTP-сервера та синхронізують системний годинник відповідно до значення часу, що отримується від нього.

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 КНЕДП "Дія".

Обов'язковому архівуванню підлягають:

- кваліфіковані сертифікати КНЕДП "Дія" 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 КНЕДП "Дія", сертифікати серверів КНЕДП "Дія" та сертифікати адміністраторів, сертифікати користувачів, а також списки відкликаних сертифікатів (CRL) зберігаються постійно.

5.5.3. Захист архіву

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

Для зберігання носіїв із резервними та архівними копіями виділяється окреме сховище (сейф чи відсік сейфа) з двома екземплярами ключів і пристроями для опечатування. Один екземпляр ключа від сховища знаходиться в адміністратора безпеки, другий в опечатаному вигляді зберігається у сховищі (сейфі) керівника профільного підрозділу КНЕДП "Дія".

Архівне приміщення обладнується технічними засобами, які виключають можливість проникнення сторонніх осіб та неконтрольованого доступу до інформації, що підлягає архівуванню. Архівні документи користувачів КНЕДП "Дія" зберігаються в спеціалізованій компанії за договором з дотриманням всіх вимог безпеки. Договірні взаємовідносини між спеціалізованою компанією та КНЕДП "Дія" здійснюються відповідно до документації СУІБ, а саме: Політики щодо інформаційної безпеки ДП «ДІЯ» з представниками сторонніх організацій DIIA/13 – ISMS – Org - PL/3 - IS Supplier relationship, затвердженої наказом від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від від 19 грудня 2023 року № 2".

5.5.4. Процедури резервного копіювання архіву

КНЕДП "Дія" забезпечує резервне копіювання архіву згідно із вимогами та інструкціями на ІКС КНЕДП "Дія".

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

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 сертифікатів із резервної копії здійснюється засобами центрального сервера ІКС КНЕДП "Дія" шляхом зчитування сертифікатів з останньої (актуальної) резервної копії та запису їх у базу даних сервера ІКС КНЕДП "Дія".

З'ємні носії зберігаються в конвертах чи упаковках, що опечатуються печаткою адміністратором безпеки. Водночас на упаковці зазначається обліковий номер копії. Факти створення та використання копій фіксуються в окремому журналі.

Резервні копії баз даних та журнали аудиту подій зберігаються у приміщенні ІКС КНЕДП "Дія" 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, зберігання та перевірку резервних копій відповідно до внутрішніх інструкцій та СУІБ, а саме Плану забезпечення безперервної діяльності ДП «ДІЯ» в межах області дії СУІБ DIIA/13 – ISMS – Org - PL/2 - GU/2 – SOP/1 - Business Continuity Plan, затвердженого наказом ДП «ДІЯ» від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань

впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 19 грудня 2023 року № 2.

5.5.5. Вимога щодо накладання електронних позначок часу на записи

КНЕДП "Дія" 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, спеціальних приміщеннях КНЕДП "Дія" та в спеціалізованій компанії за договором з дотриманням всіх вимог безпеки.

Вимоги до службових та спеціальних приміщення 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. КНЕДП "Дія" оприлюднює інформацію з архіву лише за рішенням суду.

5.6. Зміна ключа

Зміна пари ключів КНЕДП "Дія" та серверів ІКС КНЕДП "Дія" може бути:

- планова;
- позапланова.

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

Під час планової зміни ключів КНЕДП "Дія" застосовуються особливі вимоги зазначені в Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами.

Процедура планової зміни ключів КНЕДП "Дія" виконується у спеціальному приміщенні за участі керівника профільного підрозділу КНЕДП "Дія", адміністратора безпеки та адміністратора сертифікації в такому порядку:

- адміністратор безпеки та керівник профільного підрозділу КНЕДП "Дія" виконують генерацію нового особистого та відкритого ключа КНЕДП "Дія";
- адміністратор безпеки та адміністратор сертифікації формують запит на кваліфікований сертифікат відкритого ключа КНЕДП "Дія";
- керівник профільного підрозділу КНЕДП "Дія" ініціює процес засвідчення чинності відкритого ключа КНЕДП "Дія" 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 КНЕДП "Дія" від центрального засвідчувального органу, адміністратор безпеки вводить для використання особистий ключ КНЕДП "Дія";

- після отримання кваліфікованого сертифіката відкритого ключа КНЕДП "Дія" від центрального засвідчувального органу, новий сертифікат КНЕДП "Дія" публікується на офіційному вебсайті КНЕДП "Дія";

- поточна пара ключів КНЕДП "Дія" стає попередньою, а нова згенерована пара ключів стає поточною.

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

Після завершення строку чинності кваліфікованого сертифіката попереднього відкритого ключа КНЕДП "Дія", відповідний особистий ключ та всі його копії знищуються.

Попередній відкритий ключ КНЕДП "Дія" зберігається у кваліфікованому сертифікаті відкритого ключа КНЕДП "Дія" постійно.

Позапланова зміна пари ключів виконується у випадках компрометації або підозри на компрометацію особистих ключів КНЕДП "Дія", серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) або у разі виходу з ладу ЗКЕП (криптомодуля) з особистим ключем.

Після зміни особистих ключів КНЕДП "Дія" формує кваліфіковані сертифікати користувачів з використанням нової пари ключів КНЕДП "Дія".

Доступ до актуального кваліфікованого сертифіката КНЕДП "Дія" забезпечено на офіційному вебсайті ЦЗО за посиланням: https://czo.gov.ua/ca-registry-details?type=0&id=116.

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

КНЕДП "Дія" має план реагування на інциденти та план відновлення після аварій.

Порядок дій та реагування персоналом КНЕДП "Дія" на інциденти визначається документом СУІБ Політикою управління інцидентами інформаційної безпеки в ДП «ДІЯ» DIIA/13 – ISMS – Org - PL/4 – Incident management policy, затвердженою наказом ДП «ДІЯ» від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань

впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 19 грудня 2023 року № 2".

Процедури з управління інцидентами повинні передбачати:

- виконання заходів, визначених Порядком координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затвердженим наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 10 червня 2008 р. № 94, зареєстрованим в Міністерстві юстиції України 7 липня 2008 р. за № 603/15294;

- 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

Визначається наступними документами СУІБ Політикою управління інцидентами інформаційної безпеки в ДП «ДІЯ» DIIA/13 – ISMS – Org - PL/4 – Incident management policy та Планом забезпечення безперервної діяльності ДП «ДІЯ» в межах області дії СУІБ DIIA/13 – ISMS – Org - PL/2 - GU/2 – SOP/1 - Business Continuity Plan, затвердженими наказом ДП «ДІЯ» від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 19 грудня 2023 року № 2".

5.7.3. Процедури відновлення після компрометації ключа

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

У разі підтвердження факту компрометації особистого ключа КНЕДП "Дія", керівник профільного підрозділу КНЕДП "Дія" та адміністратор безпеки повинні вжити такі заходи:

- зупинити роботу мережних криптомодулів з скомпрометованими особистими ключами КНЕДП "Дія" або його серверів;

- повідомити ЦЗО про компрометацію особистого ключа КНЕДП "Дія";

- скасувати кваліфікований сертифікат КНЕДП "Дія", що відповідає скомпрометованому особистому ключу;

- ініціювати знищення скомпрометованого особистого ключа КНЕДП "Дія" у мережному криптомодулі;

- здійснити генерацію нового особистого ключа КНЕДП "Дія" та ініціювати формування для нього відповідного кваліфікованого сертифіката КНЕДП "Дія";

- ввести в дію новий особистий ключ КНЕДП "Дія" шляхом зчитування його з мережного криптомодуля.

Детальний порядок дій щодо відновлення після компрометації особистого ключа КНЕДП "Дія" визначається СУІБ .

5.7.4. Можливості безперервності бізнесу після катастрофи

КНЕДП "Дія" має резервний майданчик аналогічний основному майданчику для забезпечення безперебійності роботи у випадку аварій або катастроф відповідно до документа СУІБ Плану забезпечення безперервної діяльності ДП «ДІЯ» в межах Області дії СУІБ DIIA/13 – ISMS – Org - PL/2 - GU/2 – SOP/1 - Business Continuity Plan, затвердженого наказом ДП «ДІЯ» від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 19 грудня 2023 року № 2".

У випадку непередбаченої ситуації аварії чи катастрофи, виходу з ладу основного майданчику КНЕДП "Дія" відновлює свою роботу з резервного майданчика. Резервні копії критично важливих для відновлення роботи ІКС КНЕДП "Дія" особистих ключів, даних та інформації постійно перебувають в актуальному стані та надійно захищені.

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 КНЕДП "Дія" проводиться відповідно до затвердженого Плану припинення діяльності з надання кваліфікованих електронних довірчих послуг (далі - План припинення діяльності) з урахуванням вимог Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

5.8.1. Підстави припинення діяльності Надавача

КНЕДП "Дія" припиняє свою діяльність з надання кваліфікованих електронних довірчих послуг у разі:

1) прийняття ЦЗО рішення про скасування статусу кваліфікованого надавача;

2) прийняття КНЕДП "Дія" рішення про припинення надання кваліфікованих електронних довірчих послуг, що зазначені у Довірчому списку;

3) припинення діяльності КНЕДП "Дія" (припинення юридичної особи), крім випадків правонаступництва, визначених 5.8.4 цієї Політики сертифіката;

4) набрання законної сили рішенням суду про скасування статусу кваліфікованого надавача, визнання КНЕДП "Дія" банкрутом.

Про рішення щодо припинення надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" 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 КНЕДП "Дія" 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 вебсайті;

- надіслати до КНЕДП "Дія" повідомлення про таке рішення із зазначенням підстави його прийняття.

ЦЗО зобов’язаний оприлюднити на своєму офіційному вебсайті повідомлення про припинення надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" 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 КНЕДП "Дія" повинно містити дату публікації.

КНЕДП "Дія" припиняє діяльність з надання кваліфікованих електронних довірчих послуг через три місяці з дати оприлюднення ЦЗО на своєму офіційному вебсайті повідомлення про припинення надання КНЕДП "Дія" кваліфікованих електронних довірчих послуг.

З дати оприлюднення ЦЗО на своєму офіційному вебсайті повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" та до дати припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" зобов'язаний надавати електронні довірчі послуги, крім формування нових кваліфікованих сертифікатів.

КНЕДП "Дія", припиняючи діяльність з надання кваліфікованих електронних довірчих послуг, передає іншому надавачу 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 КНЕДП "Дія" (ДП “ДІЯ”), з іншим надавачем до закінчення терміну дії відповідного договору, КНЕДП "Дія" 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 КНЕДП "Дія" (ДП “ДІЯ”) з іншим надавачем до закінчення терміну дії відповідного договору, КНЕДП "Дія" зобов’язаний оплатити подальше надання кваліфікованих електронних довірчих послуг такому користувачеві за тарифами, встановленими відповідним надавачем.

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

У разі припинення надання кваліфікованих довірчих послуг КНЕДП "Дія" зобов’язаний передати іншому надавачу 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 КНЕДП "Дія" не пізніше дати, визначеної ним як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, або дати набрання законної сили відповідним рішенням суду.

ЦЗО скасовує виданий ним кваліфікований сертифікат КНЕДП "Дія" в день, визначений КНЕДП "Дія" 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 КНЕДП "Дія" зобов'язаний повідомити користувачам, ЦЗО та КО не пізніше п'яти робочих днів з дня прийняття такого рішення.

ЦЗО зобов'язаний оприлюднити інформацію про рішення ЦЗО щодо припинення КНЕДП "Дія" 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 вебсайті;
- надіслання до КНЕДП "Дія" повідомлення про таке рішення із зазначенням підстави його прийняття.

ЦЗО зобов'язаний опублікувати на своєму офіційному вебсайті повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" не пізніше наступного робочого дня з дня одержання повідомлення про настання підстав, передбачених підпунктами 2 - 4 пункту 5.8.1 цієї Політики сертифіката.

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

5.8.3. Дата припинення діяльності Надавача

КНЕДП "Дія" припиняє свою діяльність з надання кваліфікованих електронних довірчих послуг через три місяці з дня опублікування на своєму офіційному вебсайті ЦЗО повідомлення про припинення надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" .

З дня опублікування на своєму офіційному вебсайті ЦЗО повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" та до дня припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" зобов'язаний надавати електронні довірчі послуги, крім формування нових кваліфікованих сертифікатів.

З дня опублікування на своєму офіційному вебсайті ЦЗО повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" та до дня припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" зобов'язаний надавати електронні довірчі послуги, крім формування нових кваліфікованих сертифікатів.

ЦЗО у день, визначений як дата припинення діяльності КНЕДП "Дія" 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 КНЕДП "Дія" 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 КНЕДП "Дія" (ДП “ДІЯ”), що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, в іншого кваліфікованого надавача електронних довірчих послуг до закінчення строку дії відповідного договору КНЕДП "Дія" 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 КНЕДП "Дія" (ДП “ДІЯ”), що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, в іншого кваліфікованого надавача електронних довірчих послуг до закінчення строку дії відповідного договору, КНЕДП "Дія" 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

КНЕДП "Дія" 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 центральному засвідчувальному органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 10 жовтня 2018 р. № 821;
- 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

КНЕДП "Дія" має затверджений План припинення діяльності.

План припинення діяльності визначає умови, яких повинен дотримуватися КНЕДП "Дія" 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.

КНЕДП "Дія" 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 КНЕДП "Дія", відокремлених пунктів реєстрації, суб’єктів, які довіряють КНЕДП “Дія” 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 КНЕДП "Дія" діяльності з надання кваліфікованих електронних довірчих послуг (передача обслуговування користувачів до іншого кваліфікованого надавача).

План припинення діяльності є конфіденційним і перевіреним ООВ.

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 та документі СУІБ Положенні щодо використання засобів криптографічного захисту інформації в ДП «ДІЯ» DIIA/13 – ISMS – Tech – SOP/2 - Use of cryptography, затвердженому наказом від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 19 грудня 2023 року № 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 КНЕДП "Дія" виконується у криптографічному модулі (далі - криптомодуль) на центральному сервері ІКС КНЕДП "Дія", який знаходиться у спеціальному приміщенні, двома особами – керівником профільного підрозділу КНЕДП "Дія", адміністратором сертифікації під наглядом адміністратора безпеки.

Перед процесом генерації особистого ключа КНЕДП “Дія” здійснюється автентифікація адміністратора безпеки 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 КНЕДП "Дія" здійснюється згідно з експлуатаційною документацією на відповідний ЗКЕП ІКС КНЕДП "Дія", на яких здійснюється генерація.

Генерація пари ключів КНЕДП "Дія" та зберігання особистих ключів КНЕДП "Дія" відбувається в HSM, який використовується для випуску та зберігання ключів, що забезпечує захист від зовнішньої компрометації та працює у фізично безпечному середовищі.

Генерація пари ключів серверів КНЕДП "Дія" (OCSP, TSP, CMP) виконується на центральному сервері комплексу КНЕДП "Дія" у службовому приміщенні двома особами – адміністратором безпеки разом з адміністратором сертифікації.

Інформація щодо процедури генерації особистих ключів КНЕДП "Дія" та серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) викладено окремо в Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами, яка є невід'ємною частиною СУІБ, та належать до конфіденційної інформації, яка не підлягає оприлюдненню.

Факти генерації особистих ключів КНЕДП "Дія" та серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) заносяться до електронного журналу обліку ключових даних.

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 КНЕДП "Дія" забезпечується:

- використання користувачем виключно засобу кваліфікованого електронного підпису чи печатки та кваліфікованого сертифіката;

- захист обміну інформацією між користувачем та КНЕДП "Дія" 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 генерації ключів в офісах КНЕДП "Дія" та відокремлених пунктів реєстрації КНЕДП "Дія";

- за допомогою мобільного додатка Єдиного державного вебпорталу електронних послуг (Дія);

- за допомогою мобільного додатку, що є складовою інформаційної системи “Е-резидент”.

У разі коли пара ключів була згенерована користувачем поза приміщенням КНЕДП "Дія" та/або за відсутності відповідного персоналу, ідентифікація такого користувача, перевірка достатності обсягу його цивільної правоздатності і дієздатності, формування та видача йому кваліфікованого сертифіката здійснюється КНЕДП "Дія" 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 КНЕДП "Дія". Під час управління парою ключів користувача, 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 у вигляді апаратно-програмних засобів (захищені носії особистих ключів, токени, SIM-картки, мережні криптомодулі), 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 КНЕДП "Дія".

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).

Для надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" використовуються засоби кваліфікованого електронного підпису чи печатки, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів.

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

Надання КНЕДП "Дія" 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 вебсайт КНЕДП "Дія".

6.1.2. Доставка особистого ключа користувачу

Отримання користувачем особистого ключа у володіння в результаті надання КНЕДП "Дія" 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 КНЕДП "Дія". Не допускається формування КНЕДП "Дія" кваліфікованих сертифікатів до моменту фактичного отримання особистого ключа користувачем.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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 КНЕДП "Дія" та центрального засвідчувального органу, публікуються на вебсайті КНЕДП "Дія".

Контейнер ланцюжків сертифікатів, доступний для завантаження суб’єктами, які довіряють КНЕДП "Дія", розміщений на вебсайті КНЕДП "Дія" за посиланням: https://ca.diia.gov.ua/download-all.

Доступ до актуального кваліфікованого сертифіката КНЕДП "Дія" забезпечено на офіційному вебсайті ЦЗО за посиланням: https://czo.gov.ua/ca-registry-details?type=0&id=116.

6.1.5. Розміри (параметри) ключів

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

- алгоритм електронного підпису ДСТУ 4145-2002, розмір ключа - 256 біт, що відповідає ДСТУ 4145-2002;
- алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2014 (ISO/IEC 14888-3:2006; Cor 1:2007; Cor 2:2009; Amd 1:2010; Amd 1:2012, IDT);
- 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 апаратна генерація ключів генератор випадкових чисел (ГВЧ), що включає в себе статистичну перевірку виходу генератора. Статистична перевірка випадкових бітових послідовностей з апаратного ГВЧ

здійснюється відповідно до Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами. Ключі генеруються та зберігаються в апаратному мережевому криптомодулі "Гряда-301".

6.1.7. Основні цілі використання особистого ключа надавачем

Особисті ключі КНЕДП "Дія" забезпечують функціонування ІКС КНЕДП "Дія"

КНЕДП "Дія" визначає практику використання ключів КНЕДП "Дія" для підпису сертифікатів користувачів, сертифікатів серверів OCSP, CMP КНЕДП "Дія", списку відкликаних сертифікатів (CRL).

6.2. Захист особистого ключа та інженерний контроль криптографічного модуля

6.2.1. Стандарти та елементи керування криптографічним модулем

Для зберігання особистих ключів користувачів КНЕДП "Дія" використовує ЗКЕП, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів та також на флеш носіях у вигляді файлів у форматах *.dat та *.pfx.

Для зберігання особистих ключів КНЕДП "Дія" та серверів ІКС КНЕДП "Дія" використовуються мережні криптомодулі, що виконані у вигляді окремих апаратних пристроїв. Криптомодулі повинні мати документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів.

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

Доступ до особистого ключа КНЕДП "Дія" мають тільки уповноважені представники КНЕДП "Дія":

- керівник профільного підрозділу;
- адміністратор безпеки;
- адміністратор сертифікації.

Атрибути доступу (логін та пароль) до особистих ключів КНЕДП "Дія" зберігаються в опечатаних особистою печаткою відповідальної особи конверті, який зберігається в безпечному сховищі (сейфі), що розміщене в спеціальному приміщенні ЦОД КНЕДП "Дія", ключі та доступ до якого мають виключно відповідальні особи перелічені вище.

Управління особистими ключами КНЕДП "Дія" здійснюється відповідальними особами після їх автентифікації на центральному сервері КНЕДП "Дія" за їх особистими атрибутами доступу.

6.2.3. Управління особистим ключем підписувача

КНЕДП "Дія" забезпечує зберігання та захист особистих ключів користувачів, згенерованих в мережних криптомодулях Гряда-301 (високопродуктивний пристрій), які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону,

видане за результатами сертифікації таких засобів, які розміщені в спеціальних приміщеннях ЦОД, доступ до яких мають тільки відповідальні особи КНЕДП "Дія".

КНЕДП "Дія" 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 сертифікації таких засобів, на віддалених пунктах реєстрації за договором, укладеними з ними, які здійснюють реєстрацію користувачів, доступ до яких мають тільки відповідальні особи на відповідному пункті реєстрації.

6.2.4. Резервне копіювання особистого ключа

Резервне копіювання особистих ключів КНЕДП "Дія" та його серверів здійснюються адміністратором сертифікації під контролем адміністратора безпеки.

Під час резервного копіювання особистих ключів КНЕДП «Дія» створюється не менше двох резервних копій особистого ключа з криптомодуля. Кожна резервна копія особистого ключа КНЕДП "Дія" записується (за необхідності, – з розподілом таємниці) на зовнішній засіб кваліфікованого електронного підпису чи печатки, який є апаратно-програмним або апаратним пристроєм у захищеному вигляді, що забезпечує їх цілісність та конфіденційність.

Під час резервного копіювання особистих ключів серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) створюється не менше двох резервних копій кожного особистого ключа. Кожна резервна копія особистого ключа записується (за необхідності, – з розподілом таємниці) на ЗКЕП. У випадку, якщо особисті ключі серверів зберігаються не у криптомодулях, їх резервні копії створюються шляхом копіювання з основних ЗКЕП на резервні.

Факти резервного копіювання особистих ключів КНЕДП "Дія" та серверів ІКС КНЕДП "Дія" (OCSP, TSP, CMP) заносяться до електронного журналу обліку ключових даних.

6.2.5. Архівація особистого ключа

Особисті ключі КНЕДП "Дія" та користувачів архівуються відповідно до Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами до ІКС КНЕДП "Дія" та “Положення щодо резервного копіювання даних в ДП “ДІЯ” DIIA/13-ISMS-Tech-GU/2 - SOP/1 - Information backup, затвердженої наказом від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 19 грудня 2023 року № 2".

Після скасування або завершення строку дії кваліфікованих сертифікатів користувачів особистий ключ користувача, що зберігається в мережному криптомодулі Гряда-301 (високопродуктивний пристрій) КНЕДП "Дія", автоматично знищується.

Особисті ключі КНЕДП "Дія"” та його серверів знищуються відповідальними особами КНЕДП "Дія" після закінчення строку дії відповідних кваліфікованих сертифікатів. Факти

знищення особистих ключів КНЕДП "Дія"” та його серверів заносяться до електронного журналу обліку ключових даних.

6.2.6. Відновлення особистого ключа

Відновлення особистих ключів КНЕДП “Дія” та серверів (CMP, TSP, OCSP) здійснюються з резервних копій.

Факти відновлення особистих ключів КНЕДП "Дія" та серверів (CMP, TSP, OCSP) КНЕДП "Дія" з резервних копій заносяться до електронного журналу обліку ключових даних.

6.2.7. Зберігання особистого ключа в криптографічному модулі

Особисті ключі КНЕДП "Дія" та серверів ІКС КНЕДП “Дія” (CMP, TSP, OCSP) зберігаються та захищаються від несанкціонованого доступу в мережних криптомодулях, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами сертифікації таких засобів.

6.2.8. Активація особистих ключів

Введення в дію особистого ключа КНЕДП "Дія" та серверів (OCSP, CMP, TSP) виконується на центральному сервері ІКС КНЕДП "Дія" у службовому приміщенні надавача адміністратором безпеки.

Під час введення в дію особистого ключа шляхом підключення криптомодуля до центральних серверів КНЕДП "Дія" здійснюється автентифікація адміністратора безпеки у криптомодулі. В процесі введення особистого ключа КНЕДП "Дія" та серверів (OCSP, CMP, TSP) кваліфікований сертифікат КНЕДП "Дія", що містить відкритий ключ, зчитується з постійного диска центрального сервера.

6.2.9. Деактивація особистих ключів

Процедура деактивації особистих ключів КНЕДП "Дія" шляхом їх знищення визначена в пункті 6.2.10 цієї Політики сертифіката.

6.2.10. Знищення особистих ключів

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

Знищення особистих ключів КНЕДП "Дія" та серверів ІКС КНЕДП "Дія"(OCSP, TSP, CMP) 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.

Факти знищення особистих ключів КНЕДП "Дія" та серверів ІКС КНЕДП "Дія"(OCSP, TSP, CMP), а також їх резервних копій заносяться до журналу обліку ключових даних.

6.2.11. Можливості мережного криптографічного модуля

Мережний криптомодуль підтримує процедури, які охоплюють безпечне функціонування КНЕДП "Дія" (генерація, резервне копіювання, зберігання, знищення).

Усі мережні криптографічні модулі, що містять копії особистого ключа КНЕДП "Дія" та його серверів (OCSP, CMP, TSP) фізично захищені від несанкціонованого доступу.

Усі операції підписання за допомогою особистого ключа КНЕДП "Дія" виконуються в мережевому криптомодулі КНЕДП "Дія".

6.3. Інші аспекти керування парами ключів

6.3.1. Архівація відкритого ключа

Відкриті ключі, на основі яких сформовано кваліфіковані сертифікати зберігаються в базі даних КНЕДП "Дія" постійно.

6.3.2. Строки дії сертифіката та строки використання пари ключів

Строки дії особистих ключів КНЕДП "Дія" відповідають строкам чинності кваліфікованих сертифікатів відповідних їм відкритих ключів і становлять:

- для особистих ключів КНЕДП "Дія" та його серверів (OCSP, CMP, TSP) - не більше 5 років;
- для особистих ключів адміністраторів та користувачів - не більше 2 років.

6.4. Дані активації

6.4.1. Створення та встановлення даних активації

Відповідно до пункту 3.2 цієї Політики сертифіката.

6.4.2. Захист даних активації

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

КНЕДП "Дія" забезпечує захист інформаційних ресурсів від зовнішніх загроз, атак та несанкціонованого витоку інформації шляхом створення й підтримки безпечних інформаційних технологій (застосування багатофакторної автентифікації), в рамках яких доступ до інформації різних категорій організовується таким чином, що тільки уповноваженим користувачам або процесам надається можливість роботи з конкретною інформацією, доступ до якої обмежується і гарантується цілісність при її обробці у електронному вигляді, у вигляді друкованого документу або набору даних, що містяться на змінних носіях інформації з урахуванням документа СУІБ Положення щодо прийнятного

використання активів ДП «ДІЯ» DIIA/13 – ISMS – Org - PL/2 - GU/4 - SOP/1 - Acceptable use, затвердженого наказом ДП «ДІЯ» від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 19 грудня 2023 року № 3".

КНЕДП "Дія" забезпечує:

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

6.5.2. Рейтинг комп’ютерної безпеки

ІКС КНЕДП "Дія" перевіряються, інспектується визнаними ООВ та належним чином контролюються відповідно до [EN 319 401] та вимог чинного законодавства.

Після проходження процедури сертифікації на відповідність вимогам стандарту ISO/IEC 27002:2013(E) “Information security, cybersecurity and privacy protection — Information security management systems — Requirements” СУІБ ДП “ДІЯ” отримує сертифікат підтвердження відповідності. У випадку здійснення перевірок КО КНЕДП "Дія" отримує відповідний акт про проходження перевірки складений комісією з відповідними висновками за результатами перевірки.

6.6. Контроль безпеки життєвого циклу

6.6.1. Контроль розробки системи

При розробці та впровадженні ІКС КНЕДП "Дія" 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 КНЕДП "Дія" повинна передбачати застосування наступних заходів та засобів захисту інформації:

- організаційно-правові заходи, які реалізуються поза ІКС КНЕДП "Дія";
- інженерно-технічні заходи, що реалізуються поза ІКС КНЕДП "Дія";

- апаратні, програмно-апаратні та програмні засоби захисту від несанкціонованого доступу до інформації, яка обробляється і зберігається в КНЕДП "Дія".

Розробка програмного забезпечення із захисту інформації та оновлення його компонентів отримується безпосередньо від розробника. Допускається завантаження з офіційних вебсайтів розробника.

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

6.6.2. Засоби керування безпекою

Контроль за дотриманням вимог з безпеки в ІКС КНЕДП "Дія" здійснюється службою захисту інформації КНЕДП "Дія", на яку покладається забезпечення захисту інформації в ІКС.

Підтримка функціонування та обслуговування системи здійснюється адміністраторами згідно їх посадових обов'язків та положень документа СУІБ Положення про застосовність заходів захисту Системі управління інформаційною безпекою ДП «ДІЯ» DIIA/13 – ISMS – Org - SoA – Statement of Applicability (Версія 1.1.), затверджена наказом ДП "ДІЯ" від 05.06.2024 № 20240605-1 "Про затвердження документів, наданих згідно з протоколом Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 02 травня 2024 року № 5".

. Моніторинг інформації про стан функціонування ІКС КНЕДП "Дія", такої як відомості про використання апаратних ресурсів, збої, відмови та проблеми у роботі програмного забезпечення, сервісів здійснюється в автоматичному режимі. Адміністратори КНЕДП "Дія" отримують від системи моніторингу повідомлення у разі виникнення/усунення позаштатної ситуації.

6.6.3. Контроль безпеки протягом життєвого циклу

КНЕДП "Дія" гарантує, що обладнання та робочі станції адміністраторів ІКС КНЕДП "Дія" своєчасно модернізуються та мають останні оновлення безпеки.

6.7. Контроль безпеки мережі

КНЕДП "Дія" виконує всі технічні дії із забезпечення захисту в ІКС КНЕДП "Дія" відповідно до внутрішньої документації із захисту інформації та документа СУІБ Політики з проведення аудиту інформаційної безпеки і обробки невідповідностей в ДП «ДІЯ» DIIA/13 – ISMS – Org - PL/2 – GU/5 - IS guidelines internal audit ISMS, затвердженої наказом від 20.12.2023 № 20231220-3 "Про затвердження документів згідно протоколу Комісії з питань впровадження, забезпечення функціонування і постійного вдосконалення Системи управління інформаційною безпекою від 19 грудня 2023 року № 2" в тому числі використовуючи заходи з безпеки для запобігання несанкціонованій та зловмисній діяльності в мережі, захист від мережевих атак, контроль підключень, перевірку та відстеження стану всіх мережевих з'єднань, сканування та аудит подій міжмережного екрану, шлюзів захисту та всієї ІКС КНЕДП "Дія".

Міжмережний екран призначено для захисту від мережевих атак з боку зловмисників та розмежування доступу до ресурсів ІКС КНЕДП "Дія"".

Міжмережний монітор - аналітична платформа для управління подіями, журналами міжмережних екранів та формування звітності.

Шлюзи захисту – апаратні засоби, які призначено для захисту інформації, що передається каналами зв'язку між робочими станціями обслуговуючого персоналу КНЕДП "Дія", відокремленими пунктами реєстрації КНЕДП "Дія" та центральним сегментом ІКС КНЕДП "Дія", шляхом апаратної реалізації функцій криптографічного захисту інформації.

Програмний комплекс антивірусного захисту інформації, що має чинний позитивний експертний висновок у сфері технічного захисту інформації, виданий Адміністрацією Державної служби спеціального зв’язку та захисту інформації України, та забезпечує захист ІКС КНЕДП "Дія" від вірусів, зловмисних та небажаних програм.

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 КНЕДП "Дія" або може застосовувати інший метод, рівнозначний додаванню до кваліфікованої електронної позначки часу удосконаленого електронного підпису чи удосконаленої електронної печатки, за умови що він забезпечує рівнозначний рівень безпеки кваліфікованої електронної позначки часу та відповідає вимогам Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

Формування кваліфікованої електронної позначки часу здійснюється КНЕДП "Дія" за запитом користувача.

Під час формування кваліфікованої електронної позначки часу користувач та КНЕДП "Дія" за допомогою ЗКЕП вчиняють такі дії:

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

2) 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;

3) користувач передає сформований запит до КНЕДП "Дія";

4) КНЕДП "Дія" 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;

5) КНЕДП "Дія" 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 КНЕДП "Дія", накладені на кваліфіковану електронну позначку часу;

6) користувач після отримання відповіді від КНЕДП "Дія" 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 КНЕДП "Дія";
- перевіряє відповідність призначення сертифіката КНЕДП "Дія" (для формування позначки часу);
- перевіряє чинність сертифіката КНЕДП "Дія";

- 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 КНЕДП "Дія", 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 КНЕДП "Дія";

- перевіряє кваліфікований електронний підпис чи печатку, накладений на кваліфіковану електронну позначку часу за допомогою чинного (на момент формування кваліфікованої електронної позначки часу) сертифіката КНЕДП "Дія";

- 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 КНЕДП "Дія";

- використання скасованого або блокованого сертифіката КНЕДП "Дія" на момент формування кваліфікованої електронної позначки часу.

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

6.8.4. Отримання кваліфікованої електронної позначки часу надавачем

КНЕДП "Дія" отримує кваліфіковану електронну довірчу послугу з формування, перевірки та підтвердження кваліфікованої електронної позначки часу від ЦЗО.

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

Порядок синхронізації часу із Всесвітнім координованим часом (UTC) розробляється КНЕДП "Дія" та погоджується з ЦЗО.

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

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

7.1. Профілі сертифікатів

Кваліфіковані сертифікати, що формуються КНЕДП "Дія" 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 (версія 3) стандарт X.509
Серійний Номер	Номер сертифіката Значення цього поля є унікальним
Алгоритм підпису	Криптографічний алгоритм Визначає алгоритм, який використовується для підпису кваліфікованого сертифіката
Емітент	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)
Тема	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 КНЕДП "Дія", 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 КНЕДП "Дія" 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 КНЕДП "Дія", відповідає стандарту ITU-T X.509 та регламенту RFC 5280. CRL повинен мати щонайменше такі поля:

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

7.3. Профілі протоколу визначення статусу сертифіката (OCSP)

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

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

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

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

8. АУДИТ ВІДПОВІДНОСТІ ТА ІНШІ ОЦІНКИ

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

8.1. Частота або обставини оцінювання

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

КНЕДП "Дія" 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.

КНЕДП "Дія" повинен кожні 24 місяці за власний рахунок проходити процедуру оцінки відповідності для доведення того, що він та електронні довірчі послуги, які він надає, відповідають вимогам законодавства та стандартів.

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

КНЕДП "Дія" проходить оцінку відповідності згідно з вимогами:

- ДСТУ ETSI EN 319 401;
- ДСТУ ETSI EN 319 411-1;
- ДСТУ ETSI EN 319 411-2.

Сертифікат підтвердження відповідності ІКС КНЕДП "Дія" вимогам стандарту ISO/IEC 27001:2022 “Information security, cybersecurity and privacy protection — Information security management systems — Requirements”, отриманий за результатами проходження процедури сертифікації, діє протягом визначеного в сертифікаті строку дії.

8.2. Особа/кваліфікація оцінювача

8.2.1. Вимоги до кваліфікації контролюючого органу (КО)

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

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

Перевірка здійснюється відповідно до рішення КО.

Рішення щодо проведення перевірки повинно містити:

1) найменування Адміністрації Держспецзв’язку;
2) найменування надавача,
3) місцезнаходження надавача;
4) підставу для проведення перевірки;

5) предмет перевірки;

6) дати початку та закінчення перевірки;

7) посадовий та персональний склад комісії з перевірки.

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

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

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

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

8.3. Відносини експерта з об’єктом оцінки

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

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

Члени комісії з перевірки зобов'язані:

- об'єктивно та неупереджено проводити перевірку;
- дотримуватися вимог законодавства у сферах електронної ідентифікації, електронних довірчих послуг, захисту інформації та захисту персональних даних;
- сумлінно, вчасно та якісно виконувати свої службові обов'язки та доручення голови комісії з перевірки;
- дотримуватися ділової етики у взаємовідносинах з керівником та персоналом КНЕДП "Дія";
- ознайомлювати керівника КНЕДП "Дія" чи уповноваженого ним представника з результатами перевірки;

- надавати КНЕДП "Дія" консультаційну допомогу з питань проведення перевірки;

- не розголошувати інформацію з обмеженим доступом, яка стала їм відома у зв'язку з виконанням службових обов'язків.

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

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

8.4. Теми, охоплені оцінюванням

8.4.1. Питання, що підлягають перевірці під час державного контролю

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

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

8.4.2. Питання, що підлягають перевірці під час оцінки відповідності

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

8.5. Дії, вжиті внаслідок порушення

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

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

- здійснювати виїзні та невиїзні заходи державного нагляду (контролю) за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг;
- у разі виявлення порушення вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг видавати обов’язкові для виконання приписи про усунення порушень і визначати строк усунення виявлених порушень;
- накладати на винних осіб адміністративні стягнення за порушення вимог Закону України "Про електронну ідентифікацію та електронні довірчі послуги" та інших нормативно-правових актів, прийнятих відповідно до цього Закону;
- звертатися до суду щодо застосування заходів реагування;
- виконувати інші повноваження, визначені законом.

За результатами проведення перевірок КО вживає таких заходів реагування:

1) вимагає від КНЕДП "Дія" усунення порушень вимог законодавства у сфері електронних довірчих послуг у встановлений приписом строк;

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

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

Рішення про блокування або скасування кваліфікованого сертифіката КНЕДП "Дія" КО надсилає в день його прийняття до ЦЗО;

4) надсилає до ЦЗО подання про відкликання статусу кваліфікованого надавача електронних довірчих послуг або послуги, яку надає КНЕДП "Дія", у Довірчому списку в разі:

- надання кваліфікованих електронних довірчих послуг надавачем без чинних документів, визначених законодавством, що підтверджують відповідність вимогам стандартів серії ISO у сфері СУІБ та засобів захисту інформації у її складі вимогам нормативно-правових актів у сфері технічного та криптографічного захисту інформації, або документів про відповідність за результатами процедури оцінки відповідності у сфері електронних довірчих послуг;
- надання кваліфікованих електронних довірчих послуг за відсутності у КНЕДП "Дія" 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 ІКС КНЕДП "Дія";

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

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

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

- блокування або скасування кваліфікованого сертифіката КНЕДП "Дія".

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 вимогам стандартів серії ISO у сфері СУІБ та засобів захисту інформації у її складі вимогам нормативно-правових актів у сфері технічного та криптографічного захисту інформації, або документів про відповідність за результатами процедури оцінки відповідності у сфері електронних довірчих послуг.

8.6. 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 Дія;
- 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

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

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

9. ІНШІ КОМЕРЦІЙНІ ТА ЮРИДИЧНІ ПИТАННЯ

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

9.1. Збори

9.1.1. Плата за видачу або поновлення сертифіката

За формування кваліфікованого сертифіката сплачується плата, вартість якої визначається згідно з тарифними планами на надання кваліфікованих електронних довірчих послуг КНЕДП "Дія", опублікованими на вебсайті КНЕДП "Дія" за посиланням: https://ca.diia.gov.ua.

У разі надання кваліфікованих електронних довірчих послуг через відокремлені пункти реєстрації КНЕДП "Дія" 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 “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (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

КНЕДП "Дія" 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 КНЕДП "Дія".

9.1.5. Політика відшкодування

КНЕДП "Дія" не відшкодовує сплачені рахунки, послуги по яким надані.

9.2. Фінансова відповідальність

Діяльність КНЕДП "Дія" 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, КНЕДП "Дія" 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 вебсайті КНЕДП "Дія" та не належить до конфіденційної інформації.

9.3.3. Відповідальність за захист конфіденційної інформації

КНЕДП "Дія" здійснює захист конфіденційної інформації та несе відповідальність згідно з вимогами чинного законодавства.

9.4. Конфіденційність персональної даних

9.4.1. Концепція захисту персональних даних

КНЕДП "Дія" 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

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

Керівник профільного підрозділу КНЕДП "Дія" забезпечує створення умов для безперервної особистої освіти та постійне підвищення кваліфікації персоналу КНЕДП "Дія" 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" КНЕДП "Дія" 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

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

Керівник профільного підрозділу КНЕДП "Дія" та персонал КНЕДП "Дія" 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 КНЕДП "Дія" врегульовані відповідно до вимог чинного законодавства України.

9.6. Зобов’язання та гарантії

9.6.1. Зобов’язання та гарантії Надавача

КНЕДП "Дія" 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 КНЕДП "Дія" (ДП “ДІЯ”), реєстрацію користувачів здійснюють відокремлені пункти реєстрації КНЕДП "Дія", які виконують свої функції згідно з цією Політикою сертифіката та відповідними Положеннями сертифікаційних практик.

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

9.6.3. Зобов’язання та гарантії користувачів

КНЕДП "Дія" забезпечує можливість користувачів підписувати та перевіряти підписані файли за допомогою віджетів підписання та перевірки підписів, та за допомогою спеціалізованого програмного забезпечення, що розміщені на веб-сайті https://ca.diia.gov.ua.

Користувачі зобов'язані:

- забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа;
- невідкладно повідомляти КНЕДП "Дія" 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 КНЕДП "Дія" та користувачем;
- своєчасно надавати КНЕДП "Дія" 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 КНЕДП "Дія" ca.diia.gov.ua.

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

Суб’єкт, який довіряє КНЕДП "Дія", повинен перевірити чинність кваліфікованого сертифіката сформованого КНЕДП "Дія" за допомогою послуг перевірки та підтвердження електронного підпису чи печатки, перед використанням кваліфікованого сертифіката.

9.6.5. Зобов’язання та гарантії інших учасників

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

- документа, що підтверджує відповідність системи захисту інформації КНЕДП "Дія" вимогам положень статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах»;
- документів, які підтверджують право власності та право користування КНЕДП "Дія" нежилими приміщеннями, які використовуються для розміщення всіх складових програмно-технічного комплексу, що забезпечують надання кваліфікованих електронних довірчих послуг;
- належного персоналу КНЕДП "Дія";
- документів, які підтверджують освітньо-кваліфікаційний рівень та трирічний стаж роботи за фахом персоналу КНЕДП "Дія";
- документів, які підтверджують право власності або право користування засобами кваліфікованого електронного підпису чи печатки, які використовуються КНЕДП "Дія" для надання кваліфікованих електронних довірчих послуг;
- документів, що підтверджують внесення коштів на поточний рахунок КНЕДП "Дія" із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) для забезпечення відшкодування збитків, які можуть бути заподіяні користувачам унаслідок неналежного виконання КНЕДП "Дія" 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

КНЕДП "Дія" не надає жодних гарантій щодо послуг, які ним надаються, крім тих, які були чітко визначені в пункті 9.7.1 цієї Політики сертифіката.

9.8. Обмеження відповідальності

У разі якщо КНЕДП "Дія" 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 КНЕДП "Дія" своїх зобов’язань здійснюється відповідно до вимог чинного законодавства України.

9.10. Термін дії та припинення дії

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

9.11. Індивідуальні повідомлення та комунікації з учасниками інфраструктури відкритих ключів

КНЕДП "Дія" здійснює комунікацію з учасниками інфраструктури відкритих ключів шляхом:

- розміщення повідомлень та оголошень на вебсайті КНЕДП "Дія";
- 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 КНЕДП "Дія" 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 вебсайті КНЕДП "Дія".

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

9.13. Положення щодо вирішення спорів

У випадку виникнення спорів або розбіжностей, КНЕДП "Дія" (ДП “ДІЯ”) вирішує їх шляхом переговорів та консультацій з учасниками інфраструктури відкритих ключів.

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

9.14. Застосовне право

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

9.15. Дотримання чинного законодавства

Під час надання електронних довірчих послуг КНЕДП "Дія" 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”;
- постанова Кабінету Міністрів України від 04 грудня 2019 № 1137 “Питання Єдиного державного веб порталу електронних послуг та Реєстру адміністративних послуг”;
- постанови Кабінету Міністрів України від 10 жовтня 2018 р. № 821 “Про затвердження Порядку зберігання документованої інформації та її передавання центральному засвідчувальному 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 18 грудня 2018 р. № 1215 “Про затвердження Порядку проведення процедури оцінки відповідності у сфері електронних довірчих послуг”;
- постанови Правління Національного банку України від 17 березня 2020 р. № 32 “Про затвердження Положення про Систему BankID Національного банку України”;
- 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;

- наказу Міністерства цифрової трансформації України від 28 грудня 2023 р. № Н191 “Деякі питання реалізації вимог стандартів, у тому числі щодо забезпечення сумісності”.

Додаток 2

до Регламенту роботи кваліфікованого надавача електронних довірчих послуг “Дія”

ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК
КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ “ДІЯ”
ЩОДО КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ЕЛЕКТРОННОГО ПІДПИСУ ТА ПЕЧАТКИ

Зміст

2.2. Публікація інформації

2.2.1. Публікація сертифікатів користувачів

2.2.2. Публікація сертифікатів надавача

2.2.3. Доступ до сертифікатів користувачів

2.2.4. Строк закінчення дії сертифіката

2.3. Час та періодичність публікації

2.4. Контроль доступу до репозиторію\вебсайту

3. Ідентифікація та автентифікація

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 для запитів на зміну ключів

3.4. Ідентифікація та автентифікація користувача за заявами щодо 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. Повторний ключ 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. 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 КНЕДП "Дія" для реалізації Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

Дотримання практичних дій та процедур, визначених у цих Положеннях сертифікаційних практик, є обов'язковим для керівника профільного підрозділу КНЕДП "Дія" та найманих працівників КНЕДП "Дія", 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 КНЕДП "Дія" (державним підприємством “ДІЯ”) безпосередньо чи опосередковано пов'язані з реєстрацією користувачів, формуванням та/або обслуговуванням їхніх кваліфікованих сертифікатів електронного підпису та печатки, зокрема, відокремлених пунктів реєстрації КНЕДП "Дія".

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 КНЕДП "Дія" у процесі реєстрації користувачів, формування та обслуговування кваліфікованих сертифікатів відкритих ключів КНЕДП "Дія" та користувачів, зокрема управління їх статусом (блокування, поновлення та скасування) визначається Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

Перелік усіх практичних дій та процедур щодо кваліфікованого сертифіката віддаленого кваліфікованого електронного підпису “Дія.Підпис” (“Дія ID”), які застосовуються для реалізації Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту), визначають Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів віддаленого кваліфікованого електронного підпису “Дія.Підпис” (додаток 3 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 КНЕДП "Дія" щодо кваліфікованих сертифікатів електронного підпису та печатки.

Версія: 1.0.

1.3. Учасники інфраструктури відкритих ключів

Учасники інфраструктури відкритих ключів зазначені в пункту 5.4 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

1.3.1. Надавач

КНЕДП "Дія" 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).

КНЕДП "Дія" здійснює реєстрацію користувачів самостійно та/або через відокремлені пункти реєстрації КНЕДП "Дія".

Пункт 1.3.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить додаткову інформацію.

1.3.2. Органи реєстрації

Відокремлені пункти реєстрації КНЕДП "Дія" є органами реєстрації, що представлені окремими підрозділами, позаштатними одиницями державного КНЕДП "Дія", або юридичними чи фізичними особами, які на підставі договору з КНЕДП "Дія", здійснюють реєстрацію користувачів.

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

До працівників відокремлених пунктів реєстрації КНЕДП "Дія", 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 “Дія” (додаток 1 до цього Регламенту).

1.3.3. Користувачі

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

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

Політика сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 КНЕДП "Дія" , та використовують кваліфіковані сертифікати користувачів з метою їх автентифікації, зокрема шляхом перевірки та підтвердження електронного підпису чи печатки.

1.3.5. Інші учасники

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

Політика сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 КНЕДП "Дія", дозволено використовувати для:
- автентифікації;
- створення, перевірки та підтвердження кваліфікованого електронного підпису;
- створення, перевірки та підтвердження кваліфікованої електронної печатки;
- узгодження ключів шифрування.

Усі кваліфіковані сертифікати, сформовані КНЕДП "Дія", у розширенні “qualified certificate statement” містять значення:

1.2.804.2.1.1.1.2.1 - для забезпечення електронного документообігу та автентифікації осіб в межах країни;

1.2.804.2.1.1.1.2.2 - для програмних ключів;

1.2.804.2.1.1.1.2.4 - для особистих ключів, що зберігаються в засобі кваліфікованого електронного підпису чи печатки.

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

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

Сфера використання кваліфікованого сертифіката	**Розширення сертифіката “Призначення відкритого ключа” (“keyUsage”)**
Автентифікація	digitalSignature + nonRepudiation або keyAgreement
Створення, перевірка та підтвердження кваліфікованого електронного підпису	digitalSignature + nonRepudiation
Створення, перевірка та підтвердження кваліфікованої електронної печатки	digitalSignature + nonRepudiation
Узгодження ключів шифрування	keyAgreement

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

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

У випадках, коли вимогами до деяких інформаційно-комунікаційних систем встановлено, що автентифікація в них може здійснюватися лише з використанням кваліфікованого сертифіката, особистий ключ якого було згенеровано із застосування ЗКЕП (id-etsi-qcs 4), КНЕДП "Дія" під час формування відповідного кваліфікованого сертифіката встановлює додаткове розширення “Уточнене призначення відкритого ключа” (“extendedKeyUsage”) та умовне позначення типу такого носія із його унікальним заводським номером у додаткових даних користувача для ідентифікації типу такого ЗКЕП. Таке

розширення застосовується лише в кваліфікованих сертифікатах, особисті ключі яких згенеровані відповідно до ДСТУ 4145-2002 “Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння”, затвердженого наказом Державного комітету з питань технічного регулювання та споживчої політики від 28 грудня 2002 р. № 31.

1.4.1.1. Види сертифікатів

Відповідно до цих Положень сертифікаційних практик КНЕДП "Дія" 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 КНЕДП "Дія" зі строком дії 1 або 2 роки.

1.4.2. Заборонене використання сертифіката

Не допускається використання кваліфікованого сертифіката, сформованого КНЕДП "Дія", 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 державним підприємством «ДІЯ» (далі – ДП “ДІЯ”).

ДП “ДІЯ” є зареєстрованою відповідно до законодавства юридичною особою публічного права - державним комерційним підприємством, яке засноване на державній власності та належить до сфери управління Міністерства цифрової трансформації України.

Головний офісКНЕДП "Дія" представлений функціональним підрозділом ДП «ДІЯ», що здійснює організацію надання кваліфікованих електронних довірчих послуг відокремленими пунктами реєстрації КНЕДП "Дія" та забезпечує виконання вимог законодавства до кваліфікованих надавачів електронних довірчих послуг.

Договори про надання кваліфікованих електронних довірчих послуг укладаються від імені ДП «ДІЯ» або від імені відокремленого пункту реєстрації КНЕДП "Дія".

Реквізити ДП “ДІЯ”:

- Код згідно з Єдиним державним реєстром підприємств та організацій України (ЄДРПОУ): 43395033.
- Адреса: вул. Ділова, 24, м. Київ, 03150, Україна.
- Контактний телефон: +38 (067) 258 05 20.
- Адреса електронної пошти: inbox@diia.gov.ua.

Реквізити КНЕДП "Дія":

- Адреса веб-сайту: ca.diia.gov.ua.
- Контактний телефон: +38 (067) 107 20 41.
- Адреси електронної пошти: ca@diia.gov.ua; keys@diia.gov.ua; ca@informjust.ua.

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

Ці Положення сертифікаційних практик, а також зміни до них підписуються керівником профільного підрозділу КНЕДП "Дія", який відповідає за дотримання, визначених у них практичних дій та процедур, та затверджується генеральним директором ДП “ДІЯ”.

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

1.5.2. Внесення змін до Положень сертифікаційних практик

Відповідно до пункту 9.12 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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

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
ІКС	Інформаційно-комунікаційна система
КЗІ	Криптографічний захист інформації
РНОКПП	Реєстраційний номер облікової картки платника податків
УНЗР	Унікальний номер запису в ЄДДР
CMP	Certificate Management Protocol
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

КНЕДП "Дія" через вебсайт (https://ca.diia.gov.ua) забезпечує вільний доступ до:

- відомостей про КНЕДП "Дія";
- даних про внесення відомостей про КНЕДП "Дія" до Довірчого списку;
- Політики сертифіката КНЕДП "Дія";
- відповідних Положень сертифікаційних практик КНЕДП "Дія";
- Загальних положень та умов надання кваліфікованих електронних довірчих послуг користувачам КНЕДП "Дія";
- кваліфікованих сертифікатів КНЕДП "Дія";

- переліку кваліфікованих електронних довірчих послуг, які надає КНЕДП "Дія";
- даних про засоби кваліфікованого електронного підпису чи печатки, що використовуються під час надання кваліфікованих електронних довірчих послуг КНЕДП "Дія";
- форм документів, на підставі яких надаються кваліфіковані електронні довірчі послуги
- відомостей про відокремлені пункти реєстрації КНЕДП "Дія" 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 вебсайті КНЕДП "Дія" (https://ca.diia.gov.ua).

2.2. Публікація інформації

2.2.1. Публікація сертифікатів користувачів

Адміністратор сертифікації КНЕДП "Дія" забезпечує публікацію кваліфікованих сертифікатів користувачів, згода на публікацію яких надана такими користувачами, та списків відкликаних сертифікатів (CRL) на вебсайті КНЕДП "Дія".

КНЕДП "Дія" забезпечує вільний доступ до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів через власний вебсайт (https://ca.diia.gov.ua/).

2.2.2. Публікація сертифікатів надавача

КНЕДП "Дія" забезпечує вільний доступ до інформації про кваліфіковані сертифікати КНЕДП "Дія" через власний вебсайт (https://ca.diia.gov.ua/).

Відомості про кваліфіковані сертифікати КНЕДП "Дія", 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

КНЕДП "Дія" 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

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

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

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 КНЕДП "Дія".

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\вебсайту

Кваліфіковані сертифікати КНЕДП "Дія" та користувачів, списки відкликаних сертифікатів, відповідні Положення сертифікаційних практик та Політика сертифіката доступні у репозиторії\вебсайті 24 години на добу 7 днів на тиждень.

Доступ лише для читання необмежений. Зміни у репозиторії\веб сайті здійснюються виключно КНЕДП "Дія".

Користувач може знайти інформацію про свій кваліфікований сертифікат шляхом здійснення його пошуку на веб-сайті КНЕДП "Дія" у розділі “Пошук сертифікатів” заповнивши у відповідних вкладках інформацію про РНОКПП (у разі відсутності серія (за наявності) та номер паспорта) або серійний номер кваліфікованого сертифіката.

3. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

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

3.1. Позначення

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

1) позначку (у формі, придатній для автоматизованої обробки) про те, що сертифікат виданий як кваліфікований сертифікат;

2) позначку, що сертифікат виданий в Україні;

3) ідентифікаційні дані, які однозначно визначають КНЕДП "Дія", у тому числі обов'язково найменування та код згідно з ЄДРПОУ;

4) ідентифікаційні дані, які однозначно визначають користувача , у тому числі обов'язково:

- прізвище, власне ім'я, по батькові (за наявності) підписувача та УНЗР або РНОКПП, або серію (за наявності) та номер паспорта громадянина України (для фізичних осіб, які 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);

5) значення відкритого ключа, який відповідає особистому ключу;

6) відомості про початок та закінчення строку дії кваліфікованого сертифіката;

7) серійний номер кваліфікованого сертифіката, унікальний для КНЕДП "Дія";

8) кваліфікований електронний підпис або кваліфіковану електронну печатку, створені КНЕДП "Дія";

9) відомості про місце розміщення в безоплатному доступі кваліфікованого сертифіката, з використанням якого перевіряється удосконалений електронний підпис чи печатка, передбачені підпунктом 8 цього пункту;

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

11) 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 “Дія” (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. 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)
UniqueIdentifier(UID)	Ідентифікатор користувача, якому належить кваліфікований сертифікат: - для користувачів, що є фізичними особами, для UID використовується РНОКПП або номер паспорта; - для користувачів, що є фізичними особами - підприємцями, для UID використовується РНОКПП; - для користувачів, що є юридичними особами, для UID використовується код згідно з ЄДРПОУ

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 “Дія” (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 “Дія” (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 “Дія” (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

КНЕДП "Дія" 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 КНЕДП "Дія" містить інформацію щодо методів підтвердження володіння користувачем особистим ключем.

3.2.2. Автентифікація особи

Для ідентифікації користувача, що звернувся до КНЕДП "Дія" для отримання кваліфікованих електронних довірчих послуг, КНЕДП "Дія" вимагає разом із заявою надати, а користувач надає ідентифікаційні дані, які вносяться до кваліфікованого сертифіката.

Перелік ідентифікаційних даних, які вносяться до кваліфікованого сертифіката, та механізми їх підтвердження визначається у Таблицях 3 та 4.

Таблиця 3. Ідентифікаційні дані та механізми їх підтвердження під час встановлення фізичних осіб, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката

Ідентифікаційні дані	**Обов’язковість надання ідентифікаційних даних**	**Механізми підтвердження ідентифікаційних даних**
Прізвище, ім’я, по батькові (за наявності)	Обов’язково	Документальне або електронне (паспорт, посвідка на постійне (тимчасове) місце проживання)
РНОКПП	За наявності	Документальне або електронне (облікова картка платника податків, паспорт)
Серія (за наявності), номер паспорта	Обов’язково	Документальне або електронне (паспорт)

Ідентифікаційні дані	**Обов’язковість надання ідентифікаційних даних**	**Механізми підтвердження ідентифікаційних даних**
УНЗР	За наявності	Документальне або електронне (паспорт)
Номер телефону	Обов’язково	Технічне (відтворення тексту SMS повідомлення, надісланого КНЕДП "Дія")
Адреса електронної пошти	Обов’язково	Технічне (відповідь на електронний лист, надісланий КНЕДП "Дія")
Повноваження або займана посада	На вимогу користувача про їх включення до кваліфікованого сертифіката	Документальне (документ, що засвідчує право на здійснення діяльності у визначеній сфері: посвідчення, сертифікат, наказ про призначення, свідоцтво тощо) або технічне (інформація з відповідних державних інформаційних систем (реєстрів, баз даних тощо)

Таблиця 4. Ідентифікаційні дані та механізми їх підтвердження під час встановлення юридичних осіб, уповноважені працівники яких вперше звернулися за отриманням послуги формування кваліфікованого сертифіката.

Ідентифікаційні дані	**Обов’язковість надання ідентифікаційних даних**	**Механізми підтвердження ідентифікаційних даних**
Найменування юридичної особи	Обов’язково	Документальне або технічне (отримання інформації в електронній формі з ЄДР)
Код згідно з ЄДРПОУ	Обов’язково	Документальне або технічне (отримання інформації в електронній формі з ЄДР)

Ідентифікаційні дані	Обов’язковість надання ідентифікаційних даних	Механізми підтвердження ідентифікаційних даних
Місцезнаходження	Обов’язково	Документальне або технічне (отримання інформації в електронній формі з ЄДР)

Переліки, форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги, та роз’яснення щодо їх оформлення публікуються на веб сайті КНЕДП "Дія".

Для укладання договорів про надання кваліфікованих електронних довірчих послуг КНЕДП "Дія" може отримувати від користувачів інші документи, передбачені законодавством.

Для підтвердження належного проведення процедури встановлення користувача, КНЕДП "Дія" забезпечує зберігання заяв на формування або зміну статусу кваліфікованих сертифікатів та копій документів, які надавались користувачами під час їх ідентифікації. Копії таких документів зберігаються в паперовому вигляді в архівних приміщеннях КНЕДП "Дія" або відокремлених пунктів реєстрації КНЕДП "Дія", а також в електронній формі із забезпеченням автоматичного резервного копіювання засобами ІКС КНЕДП "Дія" та ручного архівного копіювання на окремі носії інформації.

Заяви та копії документів, які використовувались під час ідентифікації користувача, засвідчуються за правилами, наведеними у Таблиці 5.

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

Форма документа	Засвідчення з боку користувача		Засвідчення з боку КНЕДП "Дія" (адміністратор реєстрації)	
	Тип підпису	Черга засвідчення	Тип підпису	Черга засвідчення
Паперова	Власноручний підпис	Перша	Штамп адміністратора реєстрації на паперових документах. Кваліфікований електронний підпис	Друга

			адміністратора реєстрації в підсистемі створення облікових записів користувачів	
Електронна	Кваліфікований електронний підпис або електронний підпис, отриманий за допомогою засобів відтворення власноручного підпису з використанням інтерактивних сенсорних дисплеїв	Перша	Кваліфікований електронний підпис адміністратора реєстрації або виїзного адміністратора реєстрації на електронному документі. Кваліфікований електронний підпис адміністратора реєстрації в підсистемі створення облікових записів користувачів	Друга

Засвідчення КНЕДП "Дія" (адміністратором реєстрації) заяв та копій документів без завершення ідентифікації користувача і без належного засвідчення ним документів не допускається.

Під час ідентифікації користувача КНЕДП "Дія" може використовувати засоби фотофіксації факту пред'явлення користувачем документів, що посвідчують особу. Збереження фотодокументів в ІКС КНЕДП "Дія" здійснюється після їх засвідчення шляхом створення кваліфікованого електронного підпису адміністратора реєстрації.

Перевірка відомостей (даних) про особу за паспортом громадянина України або іншими документами, виданими відповідно до законодавства про ЄДДР та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи, здійснюється одним із таких способів:

- без залучення додаткових пристроїв шляхом візуального зіставлення однакової інформації (значення "УНЗР", "документ № ", "дата народження", "строк дії"), яка надрукована в зоні візуальної перевірки та машинозчитувальній зоні;

- засобами Єдиного державного веб порталу електронних послуг (Портал Дія) шляхом передачі за бажанням особи електронної копії відображення в електронній формі інформації, що міститься у її паспорті громадянина України у формі картки, та/або електронної копії відображення в електронній формі інформації, що міститься в її паспорті громадянина України для виїзду за кордон, до ІКС КНЕДП "Дія";

- шляхом автоматизованого зчитування інформації з використанням апаратних та програмних засобів (зчитувачів), які мають інтерфейс, опублікований на офіційному вебсайті державного підприємства “Поліграфічний комбінат “Україна”.

Під час ідентифікації користувача за паспортом громадянина України або іншими документами, виданими відповідно до законодавства про ЄДДР та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи, здійснюється перевірка дійсності таких документів з використанням бази даних про викрадені (втрачені) документи за зверненнями громадян єдиної інформаційної системи МВС з Єдиного державного демографічного реєстру засобами єдиної інформаційної системи МВС.

3.2.3. Неперевірена інформація про користувача

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

3.2.4. Підтвердження повноважень

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

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

3.3. Ідентифікація та автентифікація за заявою на повторний ключ

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

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

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

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

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

Повторне формування кваліфікованого сертифіката користувача не продовжує строку його дії.

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

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

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

Тип операції (причина подання заяв)	Форма подання заяв	Механізми підтвердження ідентифікаційних даних
Блокування кваліфікованого сертифіката	Усна	За ключовою фразою голосової автентифікації, первинний обмін якою між користувачем та КНЕДП "Дія" здійснюється під час подання заяви про формування кваліфікованого сертифіката
	Письмова паперова	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які вперше звернулися за отриманням послуги

		формування кваліфікованого сертифіката
	Письмова електронна	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які мають чинний кваліфікований сертифікат, сформований КНЕДП "Дія"
Скасування кваліфікованого сертифіката	Письмова паперова	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката
	Письмова електронна	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які мають чинний кваліфікований сертифікат, сформований КНЕДП "Дія"
Поновлення кваліфікованого сертифіката	Письмова паперова	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката

3.5. Автентифікація при втраті засобу автентифікації

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

Автентифікація користувача здійснюється за участю консультаційного комутатора КНЕДП "Дія" шляхом надання відповіді на секретне запитання або шляхом використання іншої форми автентифікації.

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:

1. Користувач на веб-сайті КНЕДП "Дія" https://ca.diia.gov.ua оформлює заявку для отримання кваліфікованих електронних довірчих послуг в КНЕДП "Дія" або відокремленому пункті реєстрації КНЕДП "Дія" за формою встановленою КНЕДП "Дія".

2. Фізичні, юридичні особи, представники юридичних осіб під час отримання кваліфікованих електронних довірчих послуг повинні пройти первинну ідентифікацію особи за умови особистої присутності в КНЕДП "Дія" або відокремленому пункті реєстрації КНЕДП "Дія", та надати для реєстрації необхідні документи, перелік яких надходить користувачу на електронну пошту після оформлення заяви про реєстрацію та знаходиться на веб-сайті КНЕДП "Дія".

3. Після ідентифікації користувач генерує особистий ключ за допомогою засобів наданих КНЕДП "Дія" або надає запити (відкритий ключ формату PKCS#10) на формування кваліфікованого сертифіката згенеровані ним поза приміщенням КНЕДП "Дія" або відокремленим пунктом реєстрації КНЕДП "Дія" для подальшого формування кваліфікованих сертифікатів користувача.

4. Адміністратор реєстрації КНЕДП "Дія" або віддалений адміністратор реєстрації за допомогою спеціалізованого програмного забезпечення формує кваліфікований сертифікат користувача відповідно до інформації зазначеної в заяві про реєстрацію.

Перелік документів, які повинен надати користувач:

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

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

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

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

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

4) Фізична особа-нерезидент:

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

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

- заява про реєстрацію;
- оригінал паспортного документа (для ознайомлення);
- копія паспортного документа;
- оригінал облікової картки платника податків (за наявності, для ознайомлення);
- копія облікової картки платника податків (за наявності);
- копія наказу про призначення на посаду в юридичній особі - нерезиденті (за необхідності внесення до кваліфікованого сертифіката відомостей про посаду уповноваженого представника юридичної особи - нерезидента);
- оригінал свідоцтва про реєстрацію (для ознайомлення) та його завірена копія, виданого Міністерством економіки України або Міністерством фінансів України;
- копія довідки з Головного управління статистики про відомості з ЄДРПОУ;

- засвідчена копія довіреності, договору з керівником (керуючим) представництва юридичної особи - нерезидента;

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

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

4.2. Обробка запиту на формування сертифіката

Обробка запиту на формування кваліфікованого сертифіката здійснюється програмними засобами ІКС КНЕДП "Дія" 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 КНЕДП "Дія" 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 у заяві на формування кваліфікованого сертифіката;
- шляхом запису файлу із сформованим кваліфікованим сертифікатом на носій інформації, наданий користувачем;
- шляхом публікації сформованого кваліфікованого сертифіката на веб сайті КНЕДП "Дія".

4.4. Прийняття сертифіката

Користувач повинен протягом доби перевірити свої ідентифікаційні дані, внесені КНЕДП "Дія" до кваліфікованого сертифіката. КНЕДП "Дія" 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 доби невідповідності ідентифікаційних даних, внесених КНЕДП "Дія" до кваліфікованого сертифіката, користувач повинен звернутися до КНЕДП "Дія" для скасування кваліфікованого сертифіката та безкоштовного формування нового сертифіката. У разі звернення користувача після 24 годин формування кваліфікованого сертифіката здійснюється на платній основі.

У разі невідповідності ідентифікаційних даних, внесених КНЕДП "Дія" до кваліфікованого сертифіката та виявлених КНЕДП "Дія" до моменту надання сформованого кваліфікованого сертифіката користувачу, посадовою особою КНЕДП "Дія" здійснюється переформування кваліфікованого сертифіката із використанням попередньо засвідченого відкритого ключа та з дотриманням вимог щодо недопущення перевищення часу чинності особистого ключа та відповідного йому відкритого ключа більше двох років. Посадова особа, що здійснила переформування кваліфікованого сертифіката, складає акт, в якому зазначається дата та час скасування кваліфікованого сертифіката, ідентифікаційні дані користувача, що містяться в кваліфікованому сертифікаті та невідповідні ідентифікаційні дані користувача, що зазначені у заяві про формування кваліфікованого сертифіката. Акт підписується посадовою особою КНЕДП "Дія", що здійснила переформування кваліфікованого сертифіката, та долучається до документів (засвідчених в установленому порядку копій документів), що використовувалися під час встановлення особи та реєстрації користувача.

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 КНЕДП "Дія";
- цих Положень сертифікаційних практик;

- Загальних положень та умов надання кваліфікованих електронних довірчих послуг користувачам КНЕДП "Дія";
- Договору про надання кваліфікованих електронних довірчих послуг, укладеного з КНЕДП "Дія" (ДП “ДІЯ”).

Для отримання кваліфікованого сертифіката користувач повинен:

- оформити замовлення послуги на веб-сайті КНЕДП "Дія" (https://ca.diia.gov.ua) в розділі “Отримати послугу”;
- здійснити оплату за замовлену послугу;
- підготувати необхідні для отримання послуги документи (перелік необхідних документів та заява про реєстрацію надходить користувачу на e-mail, вказаний під час замовлення послуги);
- відвідати відокремлений пункт реєстрації КНЕДП "Дія", який було обрано під час замовлення послуги;
- пройти процедуру первинної ідентифікації та надати необхідні для реєстрації документи;
- згенерувати особистий ключ на носій ключової інформації (апаратно-програмний пристрій або флеш носій) та надати відкритий ключ формату PKCS#10 для формування кваліфікованого сертифіката.

Для перевірки та використання особистого ключа користувач повинен мати:

- персональний комп'ютер з установленою операційною системою Microsoft Windows XP/2003 Server/Vista/2008 Server/2012 Server/2016 Server/7/8/8.1/10/11 або Apple macOS 10.0.4 чи новішої версії;
- встановлене програмне забезпечення “ІІТ Користувач ЦСК-1” версії не нижче 1.3.1.51 чи новішої версії або веб-браузер типу Google Chrome, Mozilla Firefox, Opera.

Детальна інформація для користувача розміщується на веб-сайті КНЕДП "Дія" (https://ca.diia.gov.ua) в розділі “Питання та відповіді”.

Пункт 4.5.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 КНЕДП "Дія", повинні дотримуватися вимог законодавства у сфері електронних довірчих послуг, а також положень:

- цих Положень сертифікаційних практик;
- Політики сертифіката КНЕДП "Дія".

Пункт 4.5.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить додаткову інформацію щодо

використання відкритого ключа та кваліфікованого сертифіката суб’єктами, які довіряють КНЕДП "Дія".

4.6. Поновлення сертифіката

КНЕДП "Дія" 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 КНЕДП "Дія" 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 КНЕДП "Дія" статусу кваліфікованого сертифіката на "поновлений".

4.7. Повторне формування сертифіката

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

Програмні засоби ІКС КНЕДП "Дія" із інтегрованими засобами кваліфікованого електронного підпису чи печатки, розміщені на вебсайті КНЕДП "Дія", 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 КНЕДП "Дія".

Створення заяви про формування нового кваліфікованого сертифіката, запиту на формування нового кваліфікованого сертифіката та їх передача на обробку до ІКС КНЕДП "Дія" 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 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

КНЕДП "Дія" скасовує сформований ним кваліфікований сертифікат протягом двох годин у разі:

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

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

3) надходження до КНЕДП "Дія" 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.

КНЕДП "Дія" 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 за підписом уповноваженої особи 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 7.

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

Підстави для зміни статусу сертифіката	**Скасування**	**Блокування**	**Підтвердження підстав**
Подання користувачем заяви	+	+	Заява користувача
Смерть фізичної особи - користувача	+		Документальне підтвердження
Припинення діяльності 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

Підстави для зміни статусу сертифіката	Скасування	Блокування	Підтвердження підстав
			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 строком до 30 календарних днів.

Після блокування кваліфікованого сертифіката, користувач може протягом 30 календарних днів поновити чинність кваліфікованого сертифіката. Блокований кваліфікований сертифікат буде автоматично скасований КНЕДП "Дія", якщо протягом зазначеного строку користувач не поновить його чинність.

Заява про скасування, блокування, кваліфікованого сертифіката подається до КНЕДП "Дія" у спосіб, що забезпечує підтвердження особи - користувача.

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

КНЕДП "Дія" здійснює цілодобовий прийом та перевірку заяв користувачів про скасування та блокування їхніх кваліфікованих сертифікатів, в тому числі, з використанням інформаційних каналів, відомості про які наведено на вебсайті КНЕДП "Дія".

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

4.10. Послуга перевірки статусу сертифіката

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

4.11. Закінчення строку дії сертифіката

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

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

Користувач може звернутися до КНЕДП "Дія" 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 “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо вимог до приміщень КНЕДП "Дія" та забезпечення фізичного доступу до них.

5.2. Процедурний контроль

Пункт 5.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо довірених ролей персоналу КНЕДП "Дія"(керівник, адміністратор реєстрації, адміністратор сертифікації, адміністратор безпеки, системний адміністратор, аудитор системи) та їх функціональних

обов'язків, щодо кількості осіб, необхідних для виконання завдань, а також довірених ролей персоналу КНЕДП "Дія", що вимагають розподілу обов’язків.

5.3. Контроль персоналу

Пункт 5.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту)” містить інформацію щодо вимог до кваліфікації, досвіду та допуску персоналу КНЕДП "Дія", вимог та процедур навчання, санкцій за несанкціоновані дії, контролю відокремлених пунктів реєстрації КНЕДП "Дія", документації, яка надається персоналу КНЕДП "Дія".

5.4. Ведення журналу аудиту подій

Пункт 5.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо видів документів та даних, що підлягають архівному зберіганню, строків зберігання архіву, захисту архіву, процедур резервного копіювання архіву, вимог щодо накладання електронних позначок часу на записи, систем збирання архівів, процедур отримання та перевірки архівної інформації.

5.6. Зміна ключа

Пункт 5.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо підстав та періодичності зміни пари ключів КНЕДП "Дія", порядку використання та доступу до актуального відкритого ключа КНЕДП "Дія".

5.7. Компрометація і аварійне відновлення

Пункт 5.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо підстав припинення діяльності КНЕДП "Дія", порядку надання повідомлення про припинення діяльності, визначення дати припинення діяльності, питань правонаступництва та передачі документованої інформації, а також Плану припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП "Дія".

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 "Дія" (додаток 1 до цього Регламенту) містить інформацію щодо генерації пари ключів КНЕДП "Дія" та користувачів, доставки особистого та відкритого ключів користувачам, доставки відкритого ключа КНЕДП "Дія" суб’єктами, які довіряють КНЕДП "Дія", щодо розмірів ключів, генерації параметрів відкритого ключа КНЕДП "Дія" та перевірки якості, основних цілей використання особистих ключів КНЕДП "Дія".

6.2. Захист особистого ключа та інженерний контроль криптографічного модуля

Пункт 6.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо стандартів та елементів керування криптографічним модулем, резервного копіювання особистого ключа, архівації особистого ключа, відновлення особистого ключа, зберігання особистого ключа в криптографічному модулі, активації особистих ключів, деактивації особистих ключів, знищення особистих ключів, можливостей мережного криптографічного модуля.

6.3. Інші аспекти керування парами ключів

Пункт 6.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг "Дія" (додаток 1 до цього Регламенту) містить інформацію щодо архівації відкритого ключа КНЕДП "Дія", строків дії сертифіката та строків використання пари ключів КНЕДП "Дія".

6.4. Дані активації

Пункт 6.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (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 “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо контролю розробки ІКС КНЕДП "Дія", засобів керування безпекою в ІКС КНЕДП "Дія", контролю безпеки протягом життєвого циклу.

6.7. Контроль безпеки мережі

Пункт 6.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо формування та перевірки кваліфікованої електронної позначки часу, наслідків недійсності кваліфікованої електронної позначки часу та процедури отримання КНЕДП "Дія" 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 “Дія” (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 “Дія” (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 “Дія” (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 “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо частоти та обставин оцінювання КНЕДП "Дія".

8.2. Особа/кваліфікація оцінювача

Пункт 8.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (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 (КНЕДП "Дія").

8.4. Теми, охоплені оцінюванням

Пункт 8.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (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 “Дія” (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 “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо проведення КНЕДП "Дія" 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 КНЕДП "Дія", опублікованими на вебсайті КНЕДП "Дія" за посиланням: https://ca.diia.gov.ua.

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

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

КНЕДП "Дія" 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 КНЕДП "Дія".

9.1.5. Політика відшкодування

КНЕДП "Дія" не відшкодовує сплачені рахунки, послуги по яким надані.

9.2. Фінансова відповідальність

Пункт 9.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо фінансової відповідальності КНЕДП "Дія".

9.3. Конфіденційність ділових даних

Пункт 9.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо змісту та обсягу конфіденційної інформації, що знаходиться в розпорядженні КНЕДП "Дія", а також відповідальності за захист конфіденційної інформації.

9.4. Захист персональних даних

Пункт 9.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо концепції захисту персональних даних в КНЕДП "Дія", визначення персональних даних, а також персональних даних, що не вважаються конфіденційними, щодо відповідальності за захист персональних даних, щодо згоди на використання персональних даних та обставин розкриття персональних даних.

9.5. Права інтелектуальної власності

Питання прав інтелектуальної власності КНЕДП "Дія" врегульовані відповідно до вимог чинного законодавства України.

9.6. Заяви та гарантії

Пункт 9.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо зобов’язань та гарантій КНЕДП "Дія", відокремлених пунктів реєстрації КНЕДП "Дія", користувачів, довіряючих сторін, а також інших учасників.

9.7. Відмова від відповідальності

Пункт 9.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо відмови від гарантій КНЕДП "Дія".

9.8. Обмеження відповідальності

Пункт 9.8 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо обставин для обмеження відповідальності КНЕДП "Дія".

9.9. Збитки

Відшкодування збитків, які можуть бути завдані користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання КНЕДП "Дія" 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 КНЕДП "Дія".

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

КНЕДП "Дія" здійснює комунікацію з учасниками інфраструктури відкритих ключів шляхом:

- розміщення повідомлень та оголошень на веб сайті КНЕДП "Дія";

- 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 КНЕДП "Дія" 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 КНЕДП "Дія".

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

9.13. Положення щодо вирішення спорів

У випадку виникнення спорів або розбіжностей, КНЕДП "Дія" (ДП “ДІЯ”) вирішує їх шляхом переговорів та консультацій з учасниками інфраструктури відкритих ключів.

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

9.14. Застосовне право

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

9.15. Дотримання чинного законодавства

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

Додаток 3

до Регламенту роботи кваліфікованого надавача електронних довірчих послуг “Дія”

ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК
КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ “ДІЯ”
ЩОДО КВАЛІФІКОВАНИХ СЕРТИФІКАТІВ ВІДДАЛЕНОГО КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПИСУ
“ДІЯ.ПІДПИС”

Зміст

2.1. Репозиторій

2.2. Публікація інформації

2.2.1. Публікація сертифікатів користувачів

2.2.2. Публікація сертифікатів надавача

2.2.3. Доступ до сертифікатів користувачів

2.2.4. Строк закінчення дії сертифіката

2.3. Час та періодичність публікації

2.4. Контроль доступу до репозиторію

3. Ідентифікація та автентифікація

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 для запитів на зміну ключів

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

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

3.4. Ідентифікація та автентифікація за заявами щодо блокування

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. Повторний ключ сертифіката

4.8. Зміна сертифіката

4.9. Блокування та скасування 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

6. Технічні заходи безпеки

6.1. Генерація та встановлення пари ключів

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

8. Аудит відповідності та інші оцінки

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

1. ВСТУП

1.1. Огляд

Ці Положення сертифікаційних практик визначають перелік практичних дій та процедур щодо кваліфікованих сертифікатів віддаленого кваліфікованого електронного підпису “Дія.Підпис” (далі - кваліфіковані сертифікати "Дія.Підпис") користувачів електронних довірчих послуг, зокрема, підписувачів (далі - користувачі), які застосовуються КНЕДП "Дія" для реалізації Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

Дотримання практичних дій та процедур, визначених у цих Положеннях сертифікаційних практик, є обов'язковим для керівника профільного підрозділу КНЕДП "Дія" та найманих працівників КНЕДП "Дія", посадові обов'язки яких безпосередньо пов'язані з реєстрацією користувачів, формуванням та обслуговуванню їхніх кваліфікованих сертифікатів "Дія.Підпис" (далі - персонал), а також фізичних та юридичних осіб, які на підставі договорів укладених з КНЕДП "Дія" (державним підприємством “ДІЯ”) безпосередньо чи опосередковано пов'язані з реєстрацією користувачів, формуванням та/або обслуговуванням їхніх кваліфікованих сертифікатів “Дія.Підпис ”.

Визнання користувачами вимог, визначених у цих Положеннях сертифікаційних практик, є обов'язковою умовою та підставою для укладення з ними договору про надання кваліфікованих електронних довірчих послуг, пов’язаних з використанням віддаленого кваліфікованого електронного підпису “Дія.Підпис” (далі - договір про надання кваліфікованих електронних довірчих послуг).

Перелік усіх правил, що застосовуються КНЕДП "Дія" у процесі реєстрації користувачів, формування та обслуговування кваліфікованих сертифікатів відкритих ключів КНЕДП "Дія" та кваліфікованих сертифікатів “Дія.Підпис” користувачів, зокрема управління їх статусом (блокування, поновлення та скасування) визначається Політикою сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

Перелік усіх практичних дій та процедур щодо кваліфікованих сертифікатів електронного підпису та печатки, які застосовуються для реалізації Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту), визначають Положення сертифікаційних практик кваліфікованого надавача

електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до цього Регламенту).

Ці Положення сертифікаційних практик відповідають вимогам, визначеним у:

- ДСТУ ETSI EN 319 401 (ETSI EN 319 401, IDT) “Електронні підписи та інфраструктури (ESI). Загальні вимоги щодо політики для надавачів довірчих послуг” (далі - ETSI EN 319 401);
- ДСТУ ETSI EN 319 411-1 (ETSI EN 319 411-1), IDT) “Електронні підписи та інфраструктури (ESI). Вимоги щодо політики та безпеки для надавачів довірчих послуг, які видають сертифікати. Частина 1. Загальні вимоги” (далі - ETSI EN 319 411-1);
- ДСТУ ETSI EN 319 411-2 (ETSI EN 319 411-2, 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 - ETSI EN 319 411-2).

1.2. Назва документа та його ідентифікація

Згідно з положеннями пункту 5.3 ETSI EN 319 411-1 та пункту 5.3 ETSI EN 319 411-2.

Повна назва	Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Дія” щодо кваліфікованих сертифікатів віддаленого кваліфікованого електронного підпису “Дія.Підпис”
Скорочена назва	Положення сертифікаційних практик КНЕДП "Дія" щодо кваліфікованих сертифікатів “Дія.Підпис”
Версія	1.0
OID	1.2.804.2.1.1.1.2.2
Ідентифікатор	NCP+ (пункт 5.3 (b) ETSI EN 319 411-1): Normalized Certificate Policy requiring a secure cryptographic device itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)

1.3. Учасники інфраструктури відкритих ключів

Згідно з положеннями пункту 5.4 ETSI EN 319 411-1 та пункту 5.4 ETSI EN 319 411-2.

1.3.1. Надавач

КНЕДП "Дія" 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 “Дія.Підпис”, в тому числі, управління їхнім статусом (блокування, поновлення та скасування).

КНЕДП "Дія" зобов'язаний:

- надавати користувачам всю необхідну інформацію щодо отримання та використання “Дія.Підпис”;
- отримувати в електронній формі за допомогою мобільного додатку Портал Дія (Дія) та мобільного додатку інформаційної системи “Е-резидент” заяви на отримання “Дія.Підпис” від користувачів;
- отримувати за допомогою мобільного додатку Портал Дія (Дія) та мобільного додатку інформаційної системи “Е-резидент” електронні копії документів та фотозображення користувачів, які подали запит на отримання “Дія.Підпис”;
- на основі отриманих від мобільного додатку Порталу Дія (Дія) та мобільного додатку інформаційної системи “Е-резидент” інформації та завірених документів формувати кваліфіковані сертифікати “Дія.Підпис” користувачів.

Пункт 1.3.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту)” містить додаткову інформацію.

1.3.2. Органи реєстрації

Відповідно до цих Положень сертифікаційних практик реєстрація користувачів здійснюється КНЕДП "Дія" віддалено, без їх особистої присутності в приміщенні КНЕДП "Дія" або відокремленому пункті реєстрації КНЕДП "Дія".

1.3.3. Користувачі

Користувачами є підписувачі, щодо яких КНЕДП "Дія" здійснює їх реєстрацію, формування та обслуговування їхніх кваліфікованих сертифікатів “Дія.Підпис”.

Користувачами можуть бути

- користувачі мобільного додатку Порталу Дія (Дія), а саме, фізичні особи яким було видано паспорт громадянина України або паспорт громадянина України для виїзду за кордон, або посвідку на постійне проживання, або посвідку на тимчасове проживання, оформлені із застосуванням засобів Єдиного державного демографічного реєстру за умови дійсності відповідного паспорта або відповідної посвідки;
- користувачі мобільного додатку Порталу Дія (Дія), а саме, представники юридичних осіб, яким було видано паспорт громадянина України або паспорт громадянина України для виїзду за кордон, або посвідку на постійне проживання, або посвідку на тимчасове проживання, оформлені із застосуванням засобів Єдиного державного демографічного реєстру, за умови дійсності відповідного паспорта або відповідної посвідки та підтвердження приналежності представника юридичної особи до юридичної особи;
- користувачі мобільного додатку інформаційної системи “Е-резидент”, а саме, фізичні особи - іноземці, які набувають статусу е-резидента та ідентифікуються за паспортним документом іноземця відповідно до постанови Кабінету Міністрів України від 05 вересня 2023 р. № 970 «Деякі питання діяльності електронних резидентів (е-резидентів) та ведення інформаційної системи «Е-резидент».

Пункт 1.3.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить додаткову інформацію.

1.3.4. Суб’єкти, які довіряють надавачу

Фізичні та юридичні особи, а також їхні інформаційно-комунікаційні системи є суб’єктами, які довіряють КНЕДП "Дія", та використовують кваліфіковані сертифікати “Дія.Підпис” користувачів з метою їх автентифікації, зокрема шляхом перевірки та підтвердження віддаленого кваліфікованого електронного підпису “Дія.Підпис”.

1.3.5. Інші учасники

Фізичні та юридичні особи, які прямо чи опосередковано пов'язані з формуванням та/або обслуговування кваліфікованих сертифікатів КНЕДП "Дія" та кваліфікованих сертифікатів “Дія.Підпис” користувачів, є іншими учасниками.

Пункт 1.3.5 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить додаткову інформацію.

1.4. Використання сертифіката

Згідно з положеннями пункту 5.5 ETSI EN 319 411-1 та пункту 5.5 ETSI EN 319 411-2.

1.4.1. Дозволене використання сертифіката

Кваліфіковані сертифікати “Дія.Підпис” можуть використовуватися в інформаційно-комунікаційних системах надання електронних послуг, в яких відповідно до законодавства повинен застосовуватися кваліфікований електронний підпис.

Кваліфіковані сертифікати “Дія.Підпис”, сформовані КНЕДП "Дія", дозволено використовувати для:

- автентифікації;
- створення, перевірки та підтвердження кваліфікованого електронного підпису “Дія.Підпис”.

Усі кваліфіковані сертифікати “Дія.Підпис”, сформовані КНЕДП "Дія", у розширенні “qualified certificate statement” містять значення “1.2.804.2.1.1.1.2.2”.

1.4.1.1. Види сертифікатів

Відповідно до цих Положень сертифікаційних практик КНЕДП “Дія” формує кваліфікований сертифікат “Дія.Підпис”, що пов'язує відкритий ключ віддаленого кваліфікованого електронного підпису “Дія.Підпис” з фізичною особою та підтверджує її ідентифікаційні дані під час автентифікації, а також створення, перевірки та підтвердження кваліфікованого електронного підпису “Дія.Підпис”.

1.4.1.2. Строк дії сертифікатів

Кваліфіковані сертифікати “Дія.Підпис” користувачів формуються КНЕДП "Дія" зі строком дії 1 рік.

1.4.2. Заборонене використання сертифіката

Не допускається використання кваліфікованого сертифіката “Дія.Підпис”, у сферах, які не відповідають зазначеному у кваліфікованому сертифікаті “Дія.Підпис” призначенню відкритого ключа (“keyUsage”).

1.5. Управління політикою

1.5.1. Відповідальність за документ

Ці Положення сертифікаційних практик підтримуються державним підприємством «ДІЯ» (далі – ДП “ДІЯ”).

ДП “ДІЯ” є зареєстрованою відповідно до законодавства юридичною особою публічного права - державним комерційним підприємством, яке засноване на державній власності та належить до сфери управління Міністерства цифрової трансформації України.

Головний офіс КНЕДП "Дія" представлений функціональним підрозділом ДП «ДІЯ».

Реквізити ДП “ДІЯ”:

- Код згідно з Єдиним державним реєстром підприємств та організацій України (ЄДРПОУ): 43395033.
- Адреса: вул. Ділова, 24, м. Київ, 03150, Україна.
- Контактний телефон: +38 (067) 258 05 20.
- Адреса електронної пошти: inbox@diia.gov.ua.

Реквізити КНЕДП "Дія":

- Адреси веб-сайтів: ca.diia.gov.ua; ca.informjust.ua.
- Контактний телефон: +38 (067) 107 20 41.
- Адреса електронної пошти: ca@diia.gov.ua.
- Ці Положення сертифікаційних практик структуровані відповідно до RFC 3647 “Інфраструктура відкритих ключів Інтернету X.509 Політика сертифікатів і практика сертифікації” і містить всю необхідну інформацію.

Ці Положення сертифікаційних практик, а також зміни до них підписуються керівником профільного підрозділу КНЕДП "Дія", який відповідає за дотримання, визначених у них практичних дій та процедур, та затверджується генеральним директором ДП “ДІЯ”.

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

1.5.2. Внесення змін до положень сертифікаційних практик

Відповідно до пункту 9.12 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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”, постановах Кабінету Міністрів України від 28.06.2024 р. № 764 “Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг”, від 04 грудня 2019 р. № 1137 “Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг”, від 05 вересня 2023 р. № 970 “Деякі питання діяльності електронних резидентів (е-резидентів) та ведення інформаційної системи “Е-резидент” (далі – Постанова про Е-резидентів), інших нормативно-правових актах у сферах електронних довірчих послуг, криптографічного та технічного захисту інформації, електронних комунікацій.

1.6.2. Перелік скорочень

Дія. Підпис	Віддалений кваліфікований електронний підпис “Дія.Підпис” (“Дія ID”), створений з використанням мобільного додатка Порталу Дія (Дія) або мобільного додатку інформаційної системи “Е-резидент”
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
ІКС	Інформаційно-комунікаційна система
Портал Дія	Єдиний державний вебпортал електронних послуг
РНОКПП	Реєстраційний номер облікової картки платника податків
УНЗР	Унікальний номер запису в ЄДДР
CRL	Certificate Revocation List (список відкликаних сертифікатів)
OCSP	Online certificate status protocol (протокол визначення статусу сертифіката)

2. ОБОВ'ЯЗКИ ЩОДО ПУБЛІКАЦІЇ ТА ЗБЕРІГАННЯ

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

2.1. Репозиторій

КНЕДП "Дія" через вебсайт (https://ca.diia.gov.ua) забезпечує вільний доступ до:

- відомостей про КНЕДП "Дія";
- даних про внесення відомостей про КНЕДП "Дія" до Довірчого списку;
- Політики сертифіката;
- відповідних Положень сертифікаційних практик;
- Загальних положень та умов надання кваліфікованих електронних довірчих послуг користувачам КНЕДП "Дія";
- кваліфікованих сертифікатів КНЕДП "Дія";
- переліку кваліфікованих електронних довірчих послуг, які надає КНЕДП "Дія";
- даних про засоби кваліфікованого електронного підпису чи печатки (QSCD), що використовуються під час надання кваліфікованих електронних довірчих послуг КНЕДП "Дія";
- форм документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;
- відомостей про відокремлені пункти реєстрації КНЕДП "Дія" 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 кваліфікованого 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 вебсайті КНЕДП "Дія" (https://ca.diia.gov.ua).

2.2. Публікація інформації

2.2.1. Публікація сертифікатів користувачів

Адміністратор сертифікації КНЕДП "Дія" забезпечує публікацію кваліфікованих сертифікатів “Дія.Підпис” користувачів, згода на публікацію яких надана такими користувачами, та списків відкликаних сертифікатів (CRL) на вебсайті КНЕДП "Дія".

КНЕДП "Дія" забезпечує вільний доступ до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів через власний вебсайт (https://ca.diia.gov.ua/).

2.2.2. Публікація сертифікатів КНЕДП "Дія"

КНЕДП "Дія" забезпечує вільний доступ до інформації про кваліфіковані сертифікати КНЕДП "Дія" через власний вебсайт (https://ca.diia.gov.ua/).

Відомості про кваліфіковані сертифікати КНЕДП "Дія", 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

КНЕДП "Дія" забезпечує цілодобовий доступ користувачів до їхніх власних кваліфікованих сертифікатів “Дія.Підпис”.

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

2.2.4. Строк закінчення дії сертифіката

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

Кваліфікований сертифікат “Дія.Підпис” вважається скасованим після настання дати та часу закінчення строку дії такого кваліфікованого сертифіката.

Строк дії кваліфікованого сертифіката “Дія.Підпис” становить один рік.

2.3. Час та періодичність публікації

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

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

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 КНЕДП "Дія".

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

Кваліфіковані сертифікати КНЕДП "Дія" та користувачів, списки відкликаних сертифікатів, відповідні Положення сертифікаційних практик та Політика сертифіката КНЕДП "Дія" доступні у репозиторії 24 години на добу 7 днів на тиждень.

Доступ лише для читання необмежений. Зміни у репозиторії та вебсайті здійснюються виключно КНЕДП "Дія"

Користувач може знайти інформацію про свій кваліфікований сертифікат “Дія.Підпис” шляхом здійснення його пошуку на веб-сайті КНЕДП "Дія" у розділі “Пошук сертифікатів”

заповнивши у відповідних вкладках інформацію про РНОКПП (у разі відсутності серія (за наявності) та номер паспорта) або серійний номер кваліфікованого сертифіката.

3. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

Згідно з положеннями пункту 6.2 ETSI EN 319 411-1 та пункту 6.2 ETSI EN 319 411-2.

3.1. Позначення

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

1) позначку (у формі, придатній для автоматизованої обробки) про те, що сертифікат виданий як кваліфікований сертифікат;

2) позначку, що сертифікат виданий в Україні;

3) ідентифікаційні дані, які однозначно визначають КНЕДП "Дія", у тому числі обов'язково найменування та код згідно з ЄДРПОУ;

4) ідентифікаційні дані, які однозначно визначають користувача:

- прізвище, власне ім’я, по батькові (за наявності) особи;
- УНЗР;
- РНОКПП (за наявності) або серія (за наявності) та номер паспорта громадянина України (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття РНОКПП та офіційно повідомили про це відповідному контролюючому органу і мають відмітку в паспорті), у разі наявності відповідної інформації в ЄДДР;
- код згідно з ЄДРПОУ (для представника юридичної особи);
- найменування юридичної особи (для представника юридичної особи);

5) значення відкритого ключа, який відповідає особистому ключу;

6) відомості про початок та закінчення строку дії кваліфікованого сертифіката;

7) серійний номер кваліфікованого сертифіката, унікальний для КНЕДП "Дія";

8) кваліфікований електронний підпис створений КНЕДП "Дія";

9) відомості про місце розміщення в безоплатному доступі кваліфікованого сертифіката, з використанням якого перевіряється удосконалений електронний підпис чи печатка, передбачені підпунктом 8 цього пункту;

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

11) 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 “Дія” (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 представника юридичної особи. Для кваліфікованих сертифікатів фізичних осіб та е-резидентів, які не належать до юридичної особи, це поле недоступне

Organizational Unit (OU)	Назва підрозділу або відділу в організації. Для кваліфікованих сертифікатів фізичних осіб та е-резидентів, які не належать до юридичної особи, це поле недоступне
State or Province (S)	Назва області місцезнаходження або місця реєстрації користувача Назва області місця реєстрації юридичної особи для кваліфікованого сертифіката представника юридичної особи
Locality (L)	Назва міста місцезнаходження або місця реєстрації користувача Назва міста реєстрації юридичної особи для кваліфікованого сертифіката представника юридичної особи
Common Name (CN)	Повне ім’я (найменування) користувача, якому належить кваліфікований сертифікат
E-Mail Address (E)	Електронна пошта користувача, якому належить кваліфікований сертифікат (за необхідності)
Title (T)	Посада (для кваліфікованих сертифікатів представників юридичної особи за необхідності)
UniqueIdentifier(UID)	Ідентифікатор користувача, якому належить кваліфікований сертифікат: ● для користувачів, що є фізичними особами, для UID використовується РНОКПП або серія (за наявності) та номер паспорта; ● для користувачів, що є юридичними особами, для UID використовується код згідно з ЄДРПОУ

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 “Дія” (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 КНЕДП "Дія".

3.1.3. Анонімність або використання псевдонімів

Не застосовується.

3.1.4. Правила інтерпретації різних форм позначень сертифіката

Міжнародні літери повинні кодуватися згідно з UTF-8.

3.1.5. Унікальність позначень сертифіката

КНЕДП "Дія" гарантує, 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

Особистий ключ кваліфікованого електронного підпису “Дія.Підпис” складається з двох частин.

Одна частина зберігається у смартфоні користувача, а інша — у засобі кваліфікованого електронного підпису, що є апаратно-програмним пристроєм, розташованим в окремому, спеціально призначеному для цього приміщенні КНЕДП "Дія".

Для підтвердження володіння особистим ключем кваліфікованого електронного підпису “Дія.Підпис” необхідно пройти підтвердження особи шляхом авторизації в

мобільному додатку Порталу Дія (Дія) або в мобільному додатку інформаційної системи “Е-резидент” та здійснення розпізнавання обличчя та введення ПІН-коду до особистого ключа кваліфікованого електронного підпису “Дія.Підпис”.

3.2.2. Автентифікація особи

3.2.2.1. Ідентифікація фізичних осіб та представників юридичних осіб

Особи, яким було видано паспорт громадянина України або паспорт громадянина України для виїзду за кордон, або посвідку на постійне проживання, або посвідку на тимчасове проживання, оформлені із застосуванням засобів ЄДДР, можуть за власним бажанням за допомогою мобільного додатка Порталу Дія (Дія), а представники юридичної особи після отримання підтвердження щодо приналежності до юридичної особи в мобільному додатку Порталу Дія (Дія), звернутися за отриманням зазначеної послуги з формування кваліфікованого сертифіката “Дія.Підпис” за умови дійсності відповідного паспорта або відповідної посвідки. Ідентифікація таких осіб здійснюється віддалено без їх особистої присутності у приміщенні КНЕДП "Дія" або у його відокремленому пункті реєстрації КНЕДП "Дія" шляхом виконання сукупності таких процедур:

1. здійснення ідентифікації особи з використанням інформації ЄДДР на підставі переданого засобами єдиної інформаційної системи МВС запиту від мобільного додатка Порталу Дія (Дія), що містить інформацію, яка дає змогу однозначно ідентифікувати особу. Запит формується на основі ідентифікаційних даних особи, переданих до мобільного додатка Порталу Дія (Дія) за допомогою Системи BankID Національного банку або зчитаних особою за допомогою мобільного додатка Порталу Дія (Дія) з безконтактного електронного носія, імплантованого у видані особі паспорт громадянина України або паспорт громадянина України для виїзду за кордон, або посвідку на постійне проживання, або посвідку на тимчасове проживання, оформлені із застосуванням засобів ЄДДР;
2. проведення перевірки дійсності виданих особі паспорта громадянина України або паспорта громадянина України для виїзду за кордон, або посвідки на постійне проживання, або посвідки на тимчасове проживання, оформлених із застосуванням засобів ЄДДР, з використанням інформації ЄДДР та бази даних про викрадені (втрачені) документи за зверненнями громадян єдиної інформаційної системи МВС на підставі переданого засобами єдиної інформаційної системи МВС запиту від мобільного додатка Порталу Дія (Дія), що містить інформацію, яка дає змогу однозначно ідентифікувати особу;
3. здійснення розпізнавання обличчя особи шляхом порівняння фотозображення особи, створеного нею за допомогою мобільного додатка Порталу Дія (Дія), з

відцифрованим образом обличчя відповідної особи, переданим з ЄДДР засобами єдиної інформаційної системи МВС до мобільного додатка Порталу Дія (Дія) (за умови надання особою ДМС однозначної згоди на обробку її персональних даних у частині передачі відцифрованого образу обличчя) або зчитаним особою за допомогою мобільного додатка Порталу Дія (Дія) з безконтактного електронного носія, імплантованого у видані особі паспорт громадянина України або паспорт громадянина України для виїзду за кордон, або посвідку на постійне проживання, або посвідку на тимчасове проживання, оформлені із застосуванням засобів ЄДДР. Розпізнавання обличчя особи здійснюється засобами мобільного додатка Порталу Дія (Дія) за умови успішного проведення перевірки на відсутність ознак атаки на біометричне пред'явлення та стороннього впливу на особу;

4. застосування додаткових механізмів для підтвердження особи.

Дані та документи, на підставі яких надаються послуги, зберігаються в архіві КНЕДП "Дія".

Пункт 5.5 Політики сертифіката КНЕДП "Дія" містить інформацію щодо видів документів та даних, що підлягають архівному зберіганню, строків зберігання архіву, захисту архіву, процедур резервного копіювання архіву, вимог щодо накладання електронних позначок часу на записи, систем збирання архівів, процедур отримання та перевірки архівної інформації.

3.2.2.2. Ідентифікація Е-резидентів

Особа, іноземець, який подав заяву про набуття статусу е-резидента та пройшов процедури перевірки, передбачені Постановою про Е-резидентів та у разі успішної ідентифікації за документами, які відображаються в інформаційній системі "Е-резидент", може самостійно за допомогою мобільного додатку інформаційної системи "Е-резидент" звернутися за отриманням послуги з формування кваліфікованого сертифіката "Дія.Підпис" за умови дійсності документів в інформаційній системі "Е-резидент".

Ідентифікація іноземців для формування кваліфікованого сертифіката "Дія.Підпис" здійснюється віддалено без їх особистої присутності у приміщенні КНЕДП "Дія" або у його відокремленому пункті реєстрації КНЕДП "Дія" шляхом виконання сукупності таких процедур:

1) здійснення верифікації особи з використанням інформаційної системи "Е-резидент" на підставі переданого запиту від мобільного додатка інформаційної системи "Е-резидент" , що містить інформацію, яка дає змогу однозначно ідентифікувати особу. Запит формується на основі ідентифікаційних даних особи, переданих до мобільного додатка інформаційної системи "Е-резидент" за допомогою інформаційної системи "Е-резидент";

2) здійснення розпізнавання обличчя особи шляхом порівняння фотографії особи, створеної нею за допомогою мобільного додатка інформаційної системи “Е-резидент” з відцифрованим образом обличчя відповідної особи, який було завантажено в інформаційну систему “Е-резидент” посадовою особою закордонної дипломатичної установи України. Розпізнавання обличчя особи здійснюється засобами мобільного додатка інформаційної системи “Е-резидент” .

До внесення відповідних змін до цих Положень сертифікаційних практик, КНЕДП "Дія" можуть використовуватись процедури ідентифікації, відмінні від визначених у цьому пункті, які оцінені та відповідно до вимог законодавства забезпечують належну ідентифікацію, за попереднім описом таких процедур ідентифікації на вебсайті КНЕДП "Дія".

Дані та документи, на підставі яких надаються послуги, зберігаються в архіві КНЕДП "Дія".

Пункт 5.5 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо видів документів та даних, що підлягають архівному зберіганню, строків зберігання архіву, захисту архіву, процедур резервного копіювання архіву, вимог щодо накладання електронних позначок часу на записи, систем збирання архівів, процедур отримання та перевірки архівної інформації.

3.2.3. Неперевірена інформація про користувача

3.2.3.1 Неперевірена інформація про користувача (фізична особа та представник юридичної особи)

Ідентифікація особи здійснюється КНЕДП "Дія" шляхом перевірки та підтвердження ідентифікаційних даних особи, отриманих КНЕДП "Дія" з ЄДДР, а для представників юридичної особи додатково отримання підтвердження щодо приналежності такої особи до юридичної особи від керівника юридичної особи або уповноваженого представника юридичної особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката “Дія.Підпис”.

Для проведення перевірки дійсності виданих особі паспорта громадянина України або паспорта громадянина України для виїзду за кордон або посвідки на постійне проживання, або посвідки на тимчасове проживання, оформлених із застосуванням засобів ЄДДР, з використанням бази даних про викрадені (втрачені) документи за зверненнями громадян єдиної інформаційної системи МВС з ЄДДР засобами єдиної інформаційної системи МВС до мобільного додатка Порталу Дія (Дія) передаються відомості про номер відповідного паспорта або відповідної посвідки.

3.2.3.2. Неперевірена інформація про користувача (е-резидент)

Ідентифікація іноземця, який подав заяву про набуття статусу е-резидента, здійснюється КНЕДП "Дія" шляхом перевірки та підтвердження ідентифікаційних даних особи, отриманих КНЕДП "Дія" з інформаційної системи “Е-резидент”, яка звернулася за отриманням послуги формування кваліфікованого сертифіката “Дія.Підпис”.

Перевірка дійсності паспортного документу іноземця, який подав заяву про набуття статусу е-резидента, здійснюється відповідно до Постанови про е-резидентів.

Формування кваліфікованого сертифіката “Дія.Підпис” іноземця, який отримав статус е-резидента, після закінчення строку використання підтверджених ідентифікаційних даних (1 рік), за умови незмінності його даних, що містяться в інформаційній системі “Е-резидент”, та у разі, коли строк дії паспортного документа закінчується не раніше ніж через три місяці, здійснюється за умови ідентифікації відповідної фізичної особи згідно з вимогами пункту 3.2.2.2 цих Положень сертифікаційних практик.

У разі коли строк дії паспортного документа закінчується менше ніж за три місяці, іноземець, який отримав статус е-резидента, має змінити паспортний документ, оновити дані в його електронному кабінеті е-резидента та пройти ідентифікацію у посадової особи закордонної дипломатичної установи України.

Іноземець після отримання нового паспортного документа, в якому його персональні дані не змінилися, повинен завантажити в електронний кабінет е-резидента копію нового паспортного документа та пройти процедуру ідентифікації, відповідно до Постанови про е-резидентів, з подальшим отриманням кваліфікованої електронної довірчої послуги з формування кваліфікованого сертифіката “Дія.Підпис”, що надається КНЕДП «Дія», на підставі нового паспортного документа з одночасним скасуванням попереднього сертифіката, чинного на даний момент часу.

Іноземець у випадку отримання нового паспортного документа, в якому змінилися персональні дані, повинен повторно пройти процедуру ідентифікації відповідно до Постанови про е-резидентів з подальшим отриманням кваліфікованої електронної довірчої послуги з формування кваліфікованого сертифіката “Дія.Підпис”, що надається КНЕДП «Дія», на підставі нового паспортного документа з одночасним скасуванням попереднього сертифіката, чинного на даний момент часу.

3.2.4. Підтвердження повноважень

КНЕДП "Дія" здійснює формування кваліфікованих сертифікатів “Дія.Підпис” для представників юридичних осіб.

Повноваження керівника та уповноваженої особи юридичної особи підтверджуються записом в ЄДРПОУ або довіреністю виданою керівником цієї юридичної особи.

Автентифікація та перевірка представників юридичних осіб здійснюється відповідно до пунктів 3.2.2.1 та 3.2.3.1 цих Положень сертифікаційних практик.

3.3. Ідентифікація та автентифікація за заявою на повторний ключ

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

3.3.1.1. Для фізичних осіб та представників юридичних осіб

Формування кваліфікованого сертифіката “Дія.Підпис” замість чинного попереднього кваліфікованого сертифіката “Дія.Підпис”, здійснюється за умови ідентифікації відповідної фізичної особи та представника юридичної особи згідно з вимогами пункту 3.2.2.1 та 3.2.3.1 цих Положень сертифікаційних практик. У такому випадку попередній кваліфікований сертифікат “Дія.Підпис” скасовується.

3.3.1.2. Для е-резидентів

Формування кваліфікованого сертифіката “Дія.Підпис” замість чинного попереднього кваліфікованого сертифіката “Дія.Підпис”, здійснюється за умови ідентифікації е-резидента згідно з вимогами пунктів 3.2.2.2 та 3.2.3.2 цих Положень сертифікаційних практик. У такому випадку попередній кваліфікований сертифікат “Дія.Підпис” скасовується.

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

Формування кваліфікованого сертифіката “Дія.Підпис” після закінчення строку використання підтверджених ідентифікаційних даних (1 рік), здійснюється за умови ідентифікації відповідної фізичної особи, представника юридичної особа та е-резидента згідно з вимогами пунктів 3.2.2 та 3.2.3 цих Положень сертифікаційних практик.

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

Ідентифікація та автентифікація користувача, під час скасування сертифіката “Дія.Підпис” здійснюється засобами мобільного додатка Порталу Дія (Дія) для фізичних осіб та представників юридичних осіб та мобільного додатка інформаційної системи “Е-резидент” для е-резидентів шляхом авторизації користувача в мобільному додатку за паролем або Face ID, які встановлені при первинній автентифікації користувача в мобільного додатку Порталу Дія (Дія) та мобільного додатка інформаційної системи “Е-резидент” відповідно до пункту 3.2.2 цих Положень сертифікаційних практик.

Скасування кваліфікованого сертифіката “Дія.Підпис” відбувається згідно з вимогами пункту 4.9 цих Положень сертифікаційних практик.

Формування кваліфікованого сертифіката “Дія.Підпис” після закінчення строку використання підтверджених ідентифікаційних даних (1 рік), здійснюється за умови ідентифікації відповідної фізичної особи згідно з вимогами пункту 3.2.2 та 3.2.3 цих Положень сертифікаційних практик.

4. ВИМОГИ ДО ЖИТТЄВОГО ЦИКЛУ СЕРТИФІКАТА

Згідно з положеннями пункту 6.3 ETSI EN 319 411-1 та пункту 6.3 ETSI EN 319 411-2.

4.1. Запит на формування сертифіката

Запит на формування кваліфікованого сертифіката можуть подати лише користувачі, визначені у пункті 1.3.3 цих Положень сертифікаційних практик, що пройшли процедури ідентифікації та автентифікації відповідно до пункту 3.2.2 та 3.2.3 цих Положень сертифікаційних практик.

4.1.1. Для фізичної особи

Процес реєстрації користувача включає в себе наступні кроки:

1) авторизація користувача в мобільному додатку Порталу Дія (Дія), що передбачає ідентифікацію та автентифікацію користувача засобами мобільному додатку Порталу Дія (Дія);
2) створення пакету документів від імені користувача, зокрема заяви про приєднання до договору про надання кваліфікованих електронних довірчих послуг, що передбачає:

- надсилання сформованого пакету документів до КНЕДП "Дія" засобами мобільного додатка Порталу Дія (Дія);
- перевірку КНЕДП "Дія" правильності сформованих документів;

3) генерація пари ключів “Дія.Підпис” користувача за допомогою мобільного додатку Порталу Дія (Дія), для чого потрібно:
   - натиснути “Створити Дія.Підпис” в меню мобільного додатку Порталу Дія (Дія);
   - підтвердити особу шляхом перевірки за фото;
   - створити 5-значний код доступу до особистого ключа “Дія.Підпис”;
   - формування КНЕДП "Дія" кваліфікованого сертифікату “Дія.Підпис” користувачу на основі отриманих ідентифікаційних даних користувача.

4.1.2. Для представників юридичних осіб

4.1.2.1. Для керівника юридичної особи

Відповідно до даних ЄДРПОУ в мобільному додатку Порталу Дія (Дія) у керівника юридичної особи відображається розділ “Юридичним особам”, в якому можливо створити “Дія.Підпис” для представника юридичної особи.

Процес реєстрації користувача (керівника) включає в себе наступні кроки:

1) авторизація користувача в мобільному додатку Порталу Дія (Дія), що передбачає ідентифікацію та автентифікацію користувача засобами мобільному додатку Порталу Дія (Дія);
2) створення пакету документів від імені користувача, зокрема заяви про приєднання до договору про надання кваліфікованих електронних довірчих послуг та її підписання, що передбачає:
   - надсилання сформованого пакету документів до КНЕДП "Дія" засобами мобільного додатка Порталу Дія (Дія);
   - перевірку КНЕДП "Дія" правильності сформованих документів;
3) генерація пари ключів “Дія.Підпис” користувача за допомогою мобільного додатку Порталу Дія (Дія), для чого потрібно:
   - натиснути “Створити Дія.Підпис” в розділі “Юридичним особам” в меню мобільного додатку Порталу Дія (Дія);
   - підтвердити особу шляхом перевірки за фото;
   - створити 5-значний код доступу до особистого ключа “Дія.Підпис” представника юридичної особи;
   - формування КНЕДП "Дія" кваліфікованого сертифікату “Дія.Підпис” керівника юридичної особи на основі отриманих ідентифікаційних даних користувача.

4.1.2.2 Для представника юридичної особи

Процес реєстрації користувача (представник юридичної особи) включає в себе наступні кроки:

1) авторизація користувача в мобільному додатку Порталу Дія (Дія), що передбачає ідентифікацію та автентифікацію користувача засобами мобільному додатку Порталу Дія (Дія);
2) отримати підтвердження приналежності до юридичної особи шляхом отримання Push-повідомлення про можливість створення “Дія.Підпис” представника юридичної особи в мобільному додатку Порталу Дія (Дія);
3) створення пакету документів від імені користувача, зокрема отримання підписаної керівником або уповноваженою особою юридичної особи заяви про приєднання до договору про надання кваліфікованих електронних довірчих послуг та її підписання, що передбачає:
    - надсилання сформованого пакету документів до КНЕДП "Дія" засобами мобільного додатка Порталу Дія (Дія);
    - перевірку КНЕДП "Дія" правильності сформованих документів;
4) генерація пари ключів “Дія.Підпис” користувача за допомогою мобільного додатку Порталу Дія (Дія), для чого потрібно:
    - натиснути “Створити Дія.Підпис” в мобільного додатку Порталу Дія (Дія);
    - підтвердити особу шляхом перевірки за фото;
    - створити 5-значний код доступу до особистого ключа “Дія.Підпис” представника юридичної особи;
    - формування КНЕДП "Дія" кваліфікованого сертифікату “Дія.Підпис” представника юридичної особи на основі отриманих ідентифікаційних даних користувача.

4.1.3. Для е-резидентів

Процес реєстрації користувача (е-резидент) включає в себе наступні кроки:

1) пройти авторизацію в мобільному додатку інформаційної системи “Е-резидент” за допомогою створеного одноразового QR-коду інформаційною системою “Е-резидент”, шляхом сканування якого користувач автентифікується в мобільному додатку інформаційної системи “Е-резидент”;
2) створення пакету документів від імені е-резидента, зокрема заяви про приєднання до договору про надання кваліфікованих електронних довірчих послуг та її підписання, що передбачає:
    - надсилання сформованого пакету документів до КНЕДП "Дія" засобами мобільного додатка інформаційної системи “Е-резидент”;
    - перевірку КНЕДП "Дія" правильності сформованих документів;

3) генерація пари ключів “Дія.Підпис” користувача за допомогою мобільного додатку Порталу Дія (Дія), для чого потрібно:
   - натиснути “Створити Дія.Підпис” в меню мобільного додатку інформаційної системи “Е-резидент”;
   - підтвердити особу шляхом перевірки за фото;
   - створити 5-значний код доступу до особистого ключа “Дія.Підпис” користувача;
   - формування КНЕДП "Дія" кваліфікованого сертифікату “Дія.Підпис” е-резидента на основі отриманих ідентифікаційних даних користувача від мобільного додатку інформаційної системи “Е-резидент”.

4.2. Обробка запиту на формування сертифіката

Обробка запиту на формування кваліфікованого сертифіката “Дія.Підпис” здійснюється програмними засобами ІКС КНЕДП "Дія" 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 здійснюється після проведення процедури ідентифікації особи користувача та підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката “Дія.Підпис”.

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

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

У випадку якщо у користувача є діючий кваліфікований сертифікат “Дія.Підпис”, він буде скасований після обробки запиту на формування нового кваліфікованого сертифіката “Дія.Підпис”.

4.3. Формування сертифіката

Надання сформованого кваліфікованого сертифіката користувачу здійснюється шляхом публікації сформованого кваліфікованого сертифіката на вебсайті КНЕДП "Дія".

4.4. Прийняття сертифіката

Користувач повинен протягом доби перевірити свої ідентифікаційні дані, внесені КНЕДП "Дія" до кваліфікованого сертифіката. КНЕДП "Дія" 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 КНЕДП "Дія" до кваліфікованого сертифіката, користувач повинен звернутися до КНЕДП "Дія" для скасування кваліфікованого сертифіката та формування нового сертифіката у порядку, встановленому цією Політикою сертифіката та відповідними Положеннями сертифікаційних практик.

У разі невідповідності ідентифікаційних даних, внесених КНЕДП "Дія" до кваліфікованого сертифіката та виявлених КНЕДП "Дія" до моменту надання сформованого кваліфікованого сертифіката користувачу, КНЕДП "Дія" здійснює переформування кваліфікованого сертифіката з дотриманням вимог щодо недопущення перевищення часу чинності особистого ключа та відповідного йому відкритого ключа більше одного року.

Користувач має можливість ознайомитись з умовами надання послуг, які розміщені на сайті КНЕДП "Дія", та викладені у:

- договорі про надання кваліфікованих електронних довірчих послуг;
- Загальних умовах та положеннях надання кваліфікованих електронних довірчих послуг користувачам кваліфікованого надавача електронних довірчих послуг “Дія”.

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 КНЕДП "Дія";
- цих Положень сертифікаційних практик;
- Загальних положень та умов надання кваліфікованих електронних довірчих послуг користувачам КНЕДП "Дія";
- Договору про надання кваліфікованих електронних довірчих послуг, укладеним з КНЕДП "Дія" (ДП “ДІЯ”).

4.5.1.1. Отримання кваліфікованого сертифіката “Дія.Підпис” фізичної особи

Для отримання кваліфікованого сертифіката “Дія.Підпис” користувач повинен:

- встановити мобільний додаток Порталу Дія (Дія) на електронному носії, критерії якого підтримують використання цього мобільного додатка (операційна система iOS 11.2 чи новішої версії або Android 4.4 чи новішої версії);
- мати паспорт громадянина України у вигляді ID-картки або паспорт громадянина України для виїзду за кордон, або посвідку на постійне проживання, або посвідку на тимчасове проживання, оформлені із застосуванням засобів ЄДДР;
- пройти авторизацію в мобільному додатку Порталу Дія (Дія) за допомогою BankID або з використанням технології NFC;
- в розділі “Меню” мобільного додатку Порталу Дія (Дія) обрати “Дія.Підпис”, ознайомитись з заявою про приєднання до Договору про надання кваліфікованих електронних довірчих послуг, яка підписується в процесі створення “Дія.Підпис”, натиснути “Активувати Дія.Підпис” та підтвердити свою особу за допомогою фото, ввести 5-ти значний цифровий код для “Дія.Підпис”.

Пункт 4.5.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) та розділ “Питання стосовно Дія.Підпис” на веб-сайті КНЕДП "Дія" містять додаткову інформацію щодо використання особистого ключа та кваліфікованого сертифіката користувачем.

4.5.1.2 Отримання кваліфікованого сертифіката “Дія.Підпис” представника юридичної особи

Для отримання кваліфікованого сертифіката "Дія.Підпис" представника юридичної особи (керівник) користувач повинен:

- встановити мобільний додаток Порталу Дія (Дія) на електронному носії, критерії якого підтримують використання цього мобільного додатка (операційна система iOS 11.2 чи новішої версії або Android 4.4 чи новішої версії);
- мати паспорт громадянина України у вигляді ID-картки або паспорт громадянина України для виїзду за кордон, або посвідку на постійне проживання, або посвідку на тимчасове проживання, оформлені із застосуванням засобів ЄДДР;
- пройти авторизацію в мобільному додатку Порталу Дія (Дія) за допомогою BankID або з використанням технології NFC;
- мати активований “Дія.Підпис”;
- в розділі “Меню” мобільного додатку Порталу Дія (Дія) обрати розділ “Юридичним особам”, який створюється відповідно до даних з ЄДРПОУ, та в ньому обрати

“Дія.Підпис”, ознайомитись з заявою про приєднання до договору про надання кваліфікованих електронних довірчих послуг, яка підписується в процесі створення “Дія.Підпис” представника юридичної особи, натиснути “Активувати “Дія.Підпис” та підтвердити свою особу за допомогою фото, ввести 5-ти значний цифровий код для “Дія.Підпис”.

Для отримання кваліфікованого сертифіката "Дія.Підпис" представника юридичної особи користувач повинен:

- встановити мобільний додаток Порталу Дія (Дія) на електронному носії, критерії якого підтримують використання цього мобільного додатка (операційна система iOS 11.2 чи новішої версії або Android 4.4 чи новішої версії);
- мати паспорт громадянина України у вигляді ID-картки або паспорт громадянина України для виїзду за кордон, або посвідку на постійне проживання, або посвідку на тимчасове проживання, оформлені із застосуванням засобів ЄДДР;
- пройти авторизацію в мобільному додатку Порталу Дія (Дія) за допомогою BankID або з використанням технології NFC;
- мати активований “Дія.Підпис”;
- отримати підтвердження приналежності юридичній особі шляхом отримання Push-повідомлення щодо можливості формування “Дія.Підпису” представника юридичної особи;
- ознайомитись та підписати заяву про приєднання до Договору, яка підписується в процесі створення “Дія.Підпис” представника юридичної особи, натиснути “Активувати “Дія.Підпис” та підтвердити свою особу за допомогою фото, ввести 5-ти значний цифровий код для “Дія.Підпис”.

Пункт 4.5.1 Політики сертифіката КНЕДП "Дія" та розділ “Питання стосовно Дія.Підпис” на веб-сайті КНЕДП "Дія" містять додаткову інформацію щодо використання особистого ключа та кваліфікованого сертифіката користувачем.

4.5.1.3. Отримання кваліфікованого сертифіката “Дія.Підпис” е-резидента

Для отримання кваліфікованого сертифіката "Дія.Підпис" користувач повинен:

- встановити мобільний додаток інформаційної системи “Е-резидент” на електронному носії, критерії якого підтримують використання цього мобільного додатка (операційна система iOS 11.2 чи новішої версії або Android 4.4 чи новішої версії);
- мати паспортний документ іноземця, який внесений в інформаційну систему “Е-резидент” відповідно до Постанови про е-резидентів;

- пройти авторизацію в мобільному додатку інформаційної системи “Е-резидент” за допомогою створеного одноразового QR-кода інформаційною системою “Е-резидент”, шляхом сканування якого користувач автентифікується в мобільному додатку інформаційної системи “Е-резидент”;
- в розділі “Меню” мобільного додатку інформаційної системи “Е-резидент” обрати “Дія.Підпис”, ознайомитись з заявою про приєднання до Договору про надання кваліфікованих електронних довірчих послуг, яка підписується в процесі створення “Дія.Підпис”, натиснути “Активувати “Дія.Підпис” та підтвердити свою особу за допомогою фото, ввести 5-ти значний цифровий код для Дія.Підпису.

Пункт 4.5.1 Політики сертифіката КНЕДП "Дія" та розділ “Питання стосовно Дія.Підпис” на веб-сайті КНЕДП "Дія" містять 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’єкти, які довіряють КНЕДП "Дія", повинні дотримуватися вимог законодавства у сфері електронних довірчих послуг, а також положень:

- цих Положень сертифікаційних практик;
- Політики сертифіката КНЕДП "Дія".

Пункт 4.5.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту)” містить додаткову інформацію щодо використання відкритого ключа та кваліфікованого сертифіката суб’єктами, які довіряють КНЕДП "Дія".

4.6. Поновлення сертифіката

Не застосовується.

Після закінчення строку чинності кваліфікованого сертифіката “Дія.Підпис” такий сертифікат автоматично скасовується, для отримання нового сертифіката “Дія.Підпис” користувач повинен пройти процедуру, передбачену пунктом 3.2.2, заново.

4.7. Повторне формування сертифіката

Формування кваліфікованого сертифіката "Дія.Підпис" після закінчення строку використання підтверджених ідентифікаційних даних (1 рік), здійснюється за умови

ідентифікації відповідної фізичної особи згідно з вимогами пункту 3.2.2 цих Положень сертифікаційних практик.

Можливе повторне (гарантійне) формування кваліфікованого сертифіката "Дія.Підпис" для представників юридичних осіб в межах чинності попередньо сформованого кваліфікованого сертифіката з урахуванням умов тарифного плану та за умови ідентифікації представників юридичних осіб згідно з вимогами пункту 3.2.2.1 цих Положень сертифікаційних практик та незмінності даних, зазначених в попередньо сформованому кваліфікованому сертифікаті.

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

КНЕДП "Дія" не пізніше ніж протягом двох годин достроково припиняє використання підтверджених ідентифікаційних даних для надання послуги з формування кваліфікованого сертифіката "Дія.Підпис" з одночасним скасуванням такого сертифіката, чинного на цей момент часу, у разі:

1) подання користувачем заяви про дострокове припинення використання підтверджених ідентифікаційних даних, що належать йому, для надання послуги з формування кваліфікованого сертифіката "Дія.Підпис" в будь-який спосіб, що забезпечує підтвердження особи користувача;

2) повідомлення користувачем або Адміністрацією Державної служби спеціального зв'язку та захисту інформації про підозру в компрометації особистого ключа, який належить користувачу;

3) надходження до КНЕДП "Дія" документа, що підтверджує:

зміну підтверджених ідентифікаційних даних;

недостовірність підтверджених ідентифікаційних даних;

смерть фізичної особи - користувача;

набрання законної сили рішенням суду про дострокове припинення використання підтверджених ідентифікаційних даних користувача для надання послуги з формування

кваліфікованого сертифіката "Дія.Підпис", оголошення фізичної особи - користувача померлою, визнання її безвісно відсутньою, недієздатною, обмеження її цивільної дієздатності, визнання її банкрутом;

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

5) розірвання договору про надання кваліфікованих електронних довірчих послуг;

6) припинення використання користувачем мобільного додатка Порталу Дія (Дія) або мобільного додатка інформаційної системи “Е-резидент”.

Відповідно до заяви про приєднання до договору про надання кваліфікованих електронних довірчих послуг користувач надає згоду на автоматичне скасування чинного кваліфікованого сертифіката "Дія.Підпис" у разі:

самостійної деактивації “Дія.Підпис” в мобільному додатку Порталу Дія (Дія) або в мобільному додатку інформаційної системи “Е-резидент”;

деактивації “Дія.Підпис” представника юридичної особи в мобільному додатку Порталу Дія (Дія) керівником юридичної особи або уповноваженим представником юридичної особи;

під час формування нового кваліфікованого сертифіката "Дія.Підпис" в мобільному додатку Порталу Дія (Дія) або в мобільному додатку інформаційної системи “Е-резидент”;

виходу із мобільного додатку Порталу Дія (Дія) або мобільного додатку інформаційної системи “Е-резидент”.

Скасовані кваліфіковані сертифікати “Дія.Підпис” потрапляють до списків відкликаних сертифікатів, що публікуються на веб-сайті КНЕДП "Дія". Частковий список відкликаних сертифікатів оновлюється кожні 2 години, Повний список відкликаних сертифікатів оновлюється 1 раз на 7 днів.

4.10. Послуга перевірки статусу сертифіката

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

КНЕДП "Дія"” забезпечує доступність інформації про статус сертифіката 24 години на добу 7 днів на тиждень.

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.

У разі необхідності дострокового припинення обслуговування кваліфікованого сертифіката “Дія.Підпис” користувач може звернутися до КНЕДП "Дія" із заявою про скасування такого сертифіката за процедурою визначеною в пункті 4.9 цих Положень сертифікаційних практик або самостійно ініціювати автоматичне скасування чинного кваліфікованого сертифіката "Дія.Підпис" у разі:

- самостійної деактивації Дія.Підпису в мобільному додатку Порталу Дія (Дія) або в мобільному додатку інформаційної системи “Е-резидент”;
- деактивації Дія.Підпису представника юридичної особи в мобільному додатку Порталу Дія (Дія) керівником юридичної особи, уповноваженим представником юридичної особи або адміністратором реєстрації за зверненням;
- під час формування нового кваліфікованого сертифіката "Дія.Підпис" в мобільному додатку Порталу Дія (Дія) або в мобільному додатку інформаційної системи “Е-резидент”;
- виходу із мобільного додатку Порталу Дія (Дія) або в мобільному додатку інформаційної системи “Е-резидент”.

4.12. Депонування та повернення ключів

Не застосовується.

5. ОБ’ЄКТ, УПРАВЛІННЯ ТА ОПЕРАЦІЙНИЙ КОНТРОЛЬ

Згідно з положеннями пункту 6.4 ETSI EN 319 411-1 та пункту 6.4 ETSI EN 319 411-2.

5.1. Контроль фізичної безпеки

Пункт 5.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо вимог до приміщень КНЕДП "Дія" та забезпечення фізичного доступу до них.

5.2. Процедурний контроль

Пункт 5.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо довірених ролей персоналу КНЕДП "Дія" (керівник, адміністратор реєстрації, адміністратор сертифікації, адміністратор безпеки, системний адміністратор, аудитор системи) та їх функціональних обов'язків, щодо кількості осіб, необхідних для виконання завдань, а також довірених ролей персоналу КНЕДП "Дія", що вимагають розподілу обов’язків.

5.3. Контроль персоналу

Пункт 5.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо вимог до кваліфікації, досвіду та допуску персоналу КНЕДП "Дія", вимог та процедур навчання, санкцій за несанкціоновані дії, контролю відокремлених пунктів реєстрації КНЕДП "Дія", документації, яка надається персоналу КНЕДП "Дія".

5.4. Ведення журналу аудиту подій

Пункт 5.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо видів документів та даних, що підлягають архівному зберіганню, строків зберігання архіву, захисту архіву, процедур резервного копіювання архіву, вимог щодо накладання електронних позначок часу на записи, систем збирання архівів, процедур отримання та перевірки архівної інформації.

5.6. Зміна ключа

Пункт 5.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо підстав та періодичності зміни пари ключів КНЕДП "Дія", порядку використання та доступу до актуального відкритого ключа КНЕДП "Дія".

5.7. Компрометація і аварійне відновлення

Пункт 5.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо підстав припинення діяльності КНЕДП "Дія", порядку надання повідомлення про припинення діяльності, визначення дати припинення діяльності, питань правонаступництва та передачі документованої інформації, а також Плану припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП "Дія".

6. ТЕХНІЧНІ ЗАХОДИ БЕЗПЕКИ

Згідно з положеннями пункту 6.5 ETSI EN 319 411-1 та пункту 6.5 ETSI EN 319 411-2.

6.1. Генерація та встановлення пари ключів

Особистий ключ у складі пари ключів користувача може бути згенерований за допомогою мобільного додатку Порталу Дія (Дія).

Під час генерації особистого ключа відбувається проходження наступних процедур:

- ідентифікація користувача засобами мобільного додатку Порталу Дія (Дія) або в мобільному додатку інформаційної системи “Е-резидент”;
- генерація пакету документів та заяви про приєднання до договору про надання кваліфікованих електронних довірчих послуг;

- надсилання сформованих документів до КНЕДП "Дія" засобами ІКС мобільного додатка Порталу Дія (Дія) або мобільного додатку інформаційної системи “Е-резидент”;
- перевірка правильності сформованих документів КНЕДП "Дія";
- генерація пари ключів користувача;
- формування кваліфікованого сертифікату користувача.

В результаті проходження цієї процедури формується особистий ключ користувача, який зберігається в хмарному сервісі КНЕДП «Дія» (мережних криптомодулях), також створюється кваліфікований сертифікат “Дія. Підпис”.

В ІКС КНЕДП "Дія" використовуються особисті та відповідні їм відкриті ключі з використанням алгоритмів електронних підписів, які визначені стандартами ДСТУ ETSI TS 119 312 “Електронні підписи та інфраструктури (ESI). Криптографічні набори” або ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння». Генерація особистого ключа КНЕДП «Дія» детально описана в пункті 6.1.1.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту).

6.2. Захист особистого ключа та інженерний контроль криптографічного модуля

Пункт 6.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо стандартів та елементів керування криптографічним модулем, резервного копіювання особистого ключа, архівації особистого ключа, відновлення особистого ключа, зберігання особистого ключа в криптографічному модулі, активації особистих ключів, деактивації особистих ключів, знищення особистих ключів, можливостей мережного криптографічного модуля.

6.3. Інші аспекти керування парами ключів

Пункт 6.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо архівації відкритого ключа КНЕДП "Дія", строків дії сертифіката та строків використання пари ключів КНЕДП "Дія".

6.4. Дані активації

Пункт 6.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (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 “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо контролю розробки ІКС КНЕДП "Дія", засобів керування безпекою в ІКС КНЕДП "Дія", контролю безпеки протягом життєвого циклу.

6.7. Контроль безпеки мережі

Пункт 6.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо формування та перевірки кваліфікованої електронної позначки часу, наслідків недійсності кваліфікованої електронної позначки часу та процедури отримання КНЕДП "Дія" кваліфікованої електронної позначки часу.

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

Згідно з положеннями пункту 6.6 ETSI EN 319 411-1 та пункту 6.6 ETSI EN 319 411-2.

7.1. Профілі сертифікатів

Пункт 7.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (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 “Дія” (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

Згідно з положеннями пункту 6.7 ETSI EN 319 411-1 та пункту 6.7 ETSI EN 319 411-2.

8.1. Частота або обставини оцінювання

Пункт 8.1 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо частоти та обставин оцінювання КНЕДП "Дія".

8.2. Особа/кваліфікація оцінювача

Пункт 8.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (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 (КНЕДП "Дія").

8.4. Теми, охоплені оцінюванням

Пункт 8.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (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 “Дія” (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 “Дія” (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 8.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо проведення КНЕДП "Дія" регулярних внутрішніх аудитів дотримання встановлених вимог.

9. ІНШІ КОМЕРЦІЙНІ ТА ЮРИДИЧНІ ПИТАННЯ

Згідно з положеннями пункту 6.8 ETSI EN 319 411-1 та пункту 6.8 ETSI EN 319 411-2.

9.1. Збори

9.1.1. Плата за видачу або поновлення сертифіката

Відповідно до постанови Кабінету Міністрів України від 4 грудня 2019 №1137 «Питання Єдиного державного веб порталу електронних послуг та Реєстру адміністративних послуг» КНЕДП "Дія" надає послугу з формування кваліфікованого сертифіката "Дія.Підпис":

- для фізичних осіб - безоплатно,
- для представників юридичних осіб - на платній основі відповідно до затверджених тарифів КНЕДП "Дія", які розміщені на вебсайті КНЕДП "Дія".
- для е-резидентів – безоплатно.

9.1.2. Плата за доступ до сертифіката

Плата за доступ до кваліфікованого сертифіката “Дія.Підпис” відсутня.

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

Плата за скасування кваліфікованого сертифіката “Дія.Підпис” або доступ до інформації про статус кваліфікованого сертифіката “Дія.Підпис” відсутня.

9.1.4. Плата за інші послуги

Формування кваліфікованого сертифіката “Дія.Підпис” не передбачає надання КНЕДП "Дія" додаткових послуг.

9.1.5. Політика відшкодування

КНЕДП "Дія" не відшкодовує сплачені рахунки, послуги по яким надані.

9.2. Фінансова відповідальність

Пункт 9.2 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо фінансової відповідальності КНЕДП "Дія".

9.3. Конфіденційність ділових даних

Пункт 9.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо змісту та обсягу конфіденційної інформації, що знаходиться в розпорядженні КНЕДП "Дія", а також відповідальності за захист конфіденційної інформації.

9.4. Захист персональних даних

Пункт 9.4 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту)” містить інформацію щодо концепції захисту персональних даних в КНЕДП "Дія", визначення персональних даних, а також персональних даних, що не вважаються конфіденційними, щодо відповідальності за захист персональних даних, щодо згоди на використання персональних даних та обставин розкриття персональних даних.

9.5. Права інтелектуальної власності

Питання прав інтелектуальної власності КНЕДП "Дія" врегульовані відповідно до вимог чинного законодавства України.

9.6. Заяви та гарантії

Пункт 9.6 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо зобов’язань та гарантій КНЕДП "Дія", відокремлених пунктів реєстрації КНЕДП "Дія", користувачів, суб’єктів, які довіряють, а також інших учасників.

9.7. Відмова від відповідальності

Пункт 9.7 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо відмови від гарантій КНЕДП "Дія".

9.8. Обмеження відповідальності

Пункт 9.8 Політики сертифіката кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо обставин для обмеження відповідальності КНЕДП "Дія".

9.9. Збитки

Відшкодування збитків, які можуть бути завдані користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання КНЕДП "Дія" 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 КНЕДП "Дія".

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

КНЕДП "Дія" здійснює комунікацію з учасниками інфраструктури відкритих ключів шляхом:

- розміщення повідомлень та оголошень на вебсайті КНЕДП "Дія";
- інформування ЦЗО, КО та органу з питань захисту персональних даних шляхом надсилання повідомлень в паперовій та електронній формах.

9.12. Зміни

Внесення змін та доповнень до цих Положень сертифікаційних практик здійснюється КНЕДП "Дія" 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 вебсайті КНЕДП "Дія".

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

9.13. Положення щодо вирішення спорів

У випадку виникнення спорів або розбіжностей, КНЕДП "Дія" (ДП “ДІЯ”) 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 кваліфікованого надавача електронних довірчих послуг “Дія” (додаток 1 до цього Регламенту) містить інформацію щодо нормативно-правових актів, які встановлюють вимоги до надання КНЕДП "Дія" кваліфікованих електронних довірчих послуг.