ЗАТВЕРДЖУЮ
Головнокомандувач Збройних Сил України
генерал-полковник

Руслан ХОМЧАК
“30” 12 2020р.

РЕГЛАМЕНТ
роботи кваліфікованого надавача електронних довірчих послуг “Центр сертифікації ключів Збройних Сил України”

ПОГОДЖЕНО
Голова Державної служби спеціального зв’язку та захисту інформації України

Юрій ЩИГОЛЬ
“23” 12 2020 р.

ПОГОДЖЕНО
Начальник Центрального управління охорони державної таємниці та захисту інформації Генерального штабу Збройних Сил України
полковник

Сергій ДУДКО
“29” 12 2020 р.

Київ 2020

ЗМІСТ

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

Регламент роботи кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України" (далі – Регламент) визначає організаційно-методологічні, технічні та технологічні умови діяльності кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України" (далі – кваліфікований надавач) та його віддалених пунктів реєстрації (далі – ВПР) під час надання кваліфікованих електронних довірчих послуг, включаючи політику сертифіката та положення сертифікаційних практик.

Регламент розроблено з урахуванням норм та положень:

Законів України "Про електронні довірчі послуги", "Про електронні документи та електронний документообіг", "Про захист персональних даних", "Про основні засади забезпечення кібербезпеки України".

Постанов Кабінету Міністрів України від 19.09.2018 року № 749 "Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності", від 07.11.2018 року № 992 "Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг"

Наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації від 14.05.2020 року № 269 "Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів та їхніх віддалених пунктів реєстрації" зареєстрованого в Міністерстві юстиції України 16.07.2020 року № 66/34951.

Інших нормативно-правових актів у сфері надання електронних довірчих послуг.

Визнання вимог Регламенту заявниками, підписувачами, створювачами електронних печаток та користувачами електронних довірчих послуг є обов'язковою умовою для отримання ними електронних довірчих послуг.

Вимоги Регламенту засновані на принципах дотримання прав та виконання обов'язків суб'єктами надання та отримання електронних довірчих послуг, які наведено в Законі України "Про електронні довірчі послуги".

Будь-яка зацікавлена особа може ознайомитися з положеннями Регламенту на офіційному електронному інформаційному ресурсі кваліфікованого надавача, безпосередньо в кваліфікованого надавача або його ВПР.

1.1 Ідентифікаційні дані кваліфікованого надавача електронних довірчих послуг.

Повне найменування: **Кваліфікований надавач електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України"**

Код ЄДРПОУ: **22991050**

Місцезнаходження: **03168, м. Київ, просп. Повітрофлотський, 6.**

Номери телефонів: **+38(044)454-41-06, (62)2-32-06, (62)2-34-78** (цілодобово, для керування статусом кваліфікованих сертифікатів відкритих ключів підписувачів).

Електронна адреса інформаційного ресурсу: **http://ca.mil.gov.ua**;

Прийом документів кваліфікованим надавачем для отримання кваліфікованих електронних довірчих послуг проводиться з 9.00 до 18.00 у робочі дні. Заявки на блокування, скасування та поновлення кваліфікованих сертифікатів відкритих ключів приймають цілодобово. Робота чергової зміни організована цілодобово, з урахуванням технологічних перерв на регламентні роботи (резервне копіювання, тощо).

1.2 Норми цього Регламенту поширюються на:

кваліфікованого надавача

ВПР кваліфікованого надавача;

посадових осіб Міністерства оборони України, Апарату Головнокомандувача Збройних Сил України, Генерального штабу Збройних Сил України, органів військового управління, вищих військових навчальних закладів, військових частин, установ, організацій Збройних Сил України та інших військових формувань, організацій, що діють в інтересах обороноздатності держави (далі – установ), які звернулись у встановленому порядку до кваліфікованого надавача чи його ВПР з метою отримання кваліфікованих електронних довірчих послуг.

Чітке дотримання та виконання умов Регламенту для вищезазначених осіб є обов'язковим.

1.3 Визначення термінів

У цьому Регламенті терміни вживаються у такому значенні:

відповідальний підрозділ (особа) за організацію використання кваліфікованих електронних довірчих послуг в установі – підрозділ, що виконує відповідні функції або посадова особа, призначена наказом керівника установи для виконання таких функцій;

володілець веб-сайту (домену) – установа власник веб-сайту, якій безпосередньо належить доменне ім'я веб-сайту (домен).

доменне ім'я (домен) – символьне позначення, яке служить для адресації вузлів мережі та мережевих ресурсів (веб-сайтів, серверів електронної пошти, мережевих серверів, тощо) в зручній для людини формі.

електронна довірча послуга - послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють кваліфікованому надавачу щодо надання такої послуги;

заявник – посадова особа (керівник установи), яка звернулася у встановленому цим Регламентом порядку до кваліфікованого надавача чи його ВПР з метою отримання кваліфікованих електронних довірчих послуги;

посадові особи – це військовослужбовці, державні службовці та працівники установ в яких наявні організаційно-розпорядчі або адміністративно-господарські функції.;

позаштатний адміністратор реєстрації – посадова особа установи, призначена наказом кваліфікованого надавача, що здійснює в установі ідентифікацію заявників, підписувачів та підтвердження володіння ними особистими ключами.

реєстрація – внесення відомостей про заявника, підписувача чи створювача електронної печатки до бази даних кваліфікованого надавача;

розпорядник веб-сайту – установа, якій володілцем веб-сайту або вищим органом військового управління поставлено завдання ведення (супроводження) веб-сайту, забезпечення роботи веб-серверу або здійснення адміністративного супроводу домену (доменного ім'я веб-сайту);

фізичні особи – це військовослужбовці, державні службовці та працівники установ.

Інші терміни та визначення, що вживаються в цьому Регламенті, визначені Законом України "Про електронні довірчі послуги" та іншими нормативно-правовими актами України у сфері електронних довірчих послуг та криптографічного захисту інформації.

1.4. Порядок затвердження і внесення змін та доповнень до Регламенту.

Регламент обов'язково погоджується з Адміністрацією Держспецзв'язку та затверджується Головнокомандувачем Збройних Сил України.

Внесення змін та доповнень до Регламенту здійснюється кваліфікованим надавачем відповідно до Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07 листопада 2018 року № 992.

Зміни та доповнення до Регламенту, що не пов'язані зі зміною чинного законодавства України, набувають чинності через 10 (десять) календарних днів з моменту розміщення зазначених змін і доповнень на електронному інформаційному ресурсі кваліфікованого надавача.

Зміни та доповнення, внесені кваліфікованим надавачем до Регламенту у зв'язку зі зміною законодавства України, набувають чинності одночасно із набранням чинності змін до відповідних нормативно-правових актів.

2 ПЕРЕЛІК ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ, НАДАННЯ ЯКИХ ЗАБЕЗПЕЧУЄ КВАЛІФІКОВАНИЙ НАДАВАЧ

2.1. Перелік кваліфікованих електронних довірчих послуг, надання яких забезпечує кваліфікований надавач

Створення, перевірка та підтвердження кваліфікованого електронного підпису чи печатки;

Формування, перевірка та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;

Формування, перевірка та підтвердження кваліфікованої електронної позначки часу.

Кожна послуга, що входить до складу електронних довірчих послуг, може надаватися як окремо, так і в сукупності.

2.2. Перелік електронних довірчих послуг, надання яких забезпечує кваліфікований надавач

Створення, перевірка та підтвердження удосконаленого електронного підпису, який базується на кваліфікованому сертифікаті відкритого ключа (надається відповідно до постанови Кабінету Міністрів України від 03.03.2020 року № 193 “ Про реалізацію експериментального проекту щодо забезпечення можливості використання удосконалених електронних підписів і печаток, які базуються на кваліфікованих сертифікатах відкритих ключів”);

Формування, перевірка та підтвердження чинності сертифіката автентифікації веб-сайту.

3 ПЕРЕЛІК ПОСАД, ОБОВЯЗКИ ЯКИХ БЕЗПОСЕРЕДНЬО ПОВЯЗАНИХ З НАДАННЯМ КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ ТА ЇХ ФУНКЦІЇ

3.1. Перелік посад, посадові обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг є:

адміністратор реєстрації;

адміністратор сертифікації;

адміністратор безпеки та аудиту;

системний адміністратор.

Перелік посад ВПР, посадові обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг є:

адміністратор реєстрації ВПР;

адміністратор безпеки та аудиту ВПР;

системний адміністратор ВПР;

адміністратор сертифікації (за необхідністю).

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

Посадові особи повинні мати необхідні для надання кваліфікованих електронних довірчих послуг знання, досвід і кваліфікацію.

Адміністратором сертифікації, адміністратором безпеки та аудиту, системним адміністратором 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.

Наявність у кваліфікованого надавача щонайменше двох посад адміністратора безпеки та аудиту.

Щорічне проходження адміністратором безпеки та аудиту практичних навчань з інформаційної безпеки, що передбачають вивчення нових загроз інформаційної безпеки та реагування на них.

З метою забезпечення вирішення питань, пов'язаних із проектуванням, розробленням і модернізацією, введенням в експлуатацію, обслуговуванням і підтримкою працездатності комплексної системи захисту інформації (далі – КСЗІ), а також протистояння узагальненій сукупності кібернетичних загроз, цілісності інформації в інформаційно-телекомунікаційних систем, які виникають при взаємодії інформаційно-телекомунікаційних систем (далі – ІТС) з користувачами через ІСД-Інтернет або автоматизованої системи управління Збройних Сил України "Дніпро" (далі – АСУ ЗСУ "Дніпро"), повноти та якісного виконання організаційних та

технічних заходів із захисту інформації та додержання режиму безпеки створено службу захисту інформації. Склад, функції та обов'язки служби захисту інформації визначені в Положенні про Службу охорони державної таємниці та захисту інформації, що затверджене командиром військової частини А0136.

3.2. Функції та відповідальність посадових осіб, які безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг:

Виконання обов'язків керівника кваліфікованого надавача покладається на командира військової частини А0136. Виконання обов'язків адміністраторів покладається на військовослужбовців військової частини А0136 відповідним наказом командира частини.

Реалізацію функцій кваліфікованого надавача з реєстрації підписувачів та їх обслуговування на визначеній території (для визначеного складу військ (сил) здійснюють ВПР, які є територіально відокремленими підрозділами кваліфікованого надавача без правового статусу юридичної особи.

Персонал, що забезпечує роботу ВПР, підпорядковується керівнику кваліфікованого надавача з питань реєстрації підписувачів та їх обслуговування.

Кваліфікований надавач та його ВПР здійснює свої повноваження в межах розподілу, визначеного Генеральним штабом Збройних Сил України.

3.2.1. Адміністратор реєстрації відповідає за перевірку документів наданих заявниками, підписувачами чи відповідальними особами, заявок про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів підписувачів.

Основними обов'язками адміністратора реєстрації є:

ідентифікація та автентифікація заявників, підписувачів та відповідальних осіб;

внесення відомостей про заявників до бази даних кваліфікованого надавача;

перевірка заявок про формування, блокування, поновлення та скасування кваліфікованих сертифікатів відкритих ключів;

встановлення належності відкритого ключа та відповідного йому особистого ключа заявнику, підписувачу;

ведення обліку підписувачів.

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

Основними обов'язками адміністратора сертифікації є:

участь у генерації пар ключів кваліфікованого надавача та створенні резервних копій особистих ключів кваліфікованого надавача;

зберігання особистих ключів кваліфікованого надавача та їх резервних копій;

забезпечення використання особистих ключів кваліфікованого надавача під час формування та обслуговування кваліфікованих сертифікатів відкритих ключів кваліфікованого надавача, підписувачів;

перевірка заявок про формування кваліфікованих сертифікатів відкритих ключів кваліфікованого надавача на відповідність вимогам Регламенту роботи кваліфікованого надавача;

участь у знищенні особистих ключів кваліфікованого надавача;

забезпечення ведення, архівування та відновлення баз даних кваліфікованих сертифікатів відкритих ключів підписувачів;

забезпечення публікації кваліфікованих сертифікатів відкритих ключів підписувачів та списків відкликаних сертифікатів на офіційному веб-сайті кваліфікованого надавача;

створення резервних копій кваліфікованих сертифікатів відкритих ключів підписувачів;

зберігання кваліфікованих сертифікатів відкритих ключів підписувачів, їх резервних копій, списків відкликаних сертифікатів та інших важливих ресурсів ІТС кваліфікованого надавача.

3.2.3. Адміністратор безпеки та аудиту відповідає за належне функціонування КСЗІ або/та системи управління інформаційною безпекою.

Основними обов'язками адміністратора безпеки та аудиту є:

участь у генерації пар ключів кваліфікованого надавача та створенні резервних копій особистих ключів кваліфікованого надавача;

контроль за формуванням, обслуговуванням і створенням резервних копій кваліфікованих сертифікатів відкритих ключів кваліфікованого надавача, підписувачів та списків відкликаних сертифікатів;

контроль за зберіганням особистих ключів кваліфікованого надавача та їх резервних копій, особистих ключів адміністраторів;

участь у знищенні особистих ключів кваліфікованого надавача, контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;

організація розмежування доступу до ресурсів ІТС кваліфікованого надавача;

забезпечення спостереження за функціонуванням КСЗІ або системи управління інформаційною безпекою (реєстрація подій в ІТС кваліфікованого надавача, моніторинг подій тощо);

забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ або системи управління інформаційною безпекою після збоїв, відмов, аварій ІТС кваліфікованого надавача;

забезпечення режиму доступу до приміщень кваліфікованого надавача, в яких розміщена ІТС кваліфікованого надавача;

ведення журналів обліку адміністратора безпеки та аудиту, визначених документацією на КСЗІ або звітності, що передбачена системою управління інформаційною безпекою;

проведення перевірок журналів аудиту подій, що реєструють технічні засоби ІТС кваліфікованого надавача;

проведення перевірок відповідності положень внутрішньої організаційно-розпорядчої документації кваліфікованого надавача та документації на КСЗІ або систему управління інформаційною безпекою;

контроль за дотриманням посадовими особами кваліфікованого надавача положень внутрішньої організаційно-розпорядчої документації кваліфікованого надавача та документації щодо КСЗІ або системи управління інформаційною безпекою;

контроль за веденням баз даних кваліфікованого надавача;

контроль за веденням архіву кваліфікованого надавача.

Адміністратор безпеки та аудиту відповідає за проведення перевірок дотримання посадовими особами, які виконують обов'язки пов'язані з наданням кваліфікованих електронних довірчих послуг кваліфікованого надавача положень внутрішньої організаційно-розпорядчої документації кваліфікованого надавача та документації щодо КСЗІ та/або системи управління інформаційною безпекою.

3.2.4. Системний адміністратор відповідає за функціонування засобів та обладнання програмно-технічного комплексу кваліфікованого надавача (далі — ПТК) ІТС кваліфікованого надавача.

Основними обов'язками системного адміністратора є:

організація експлуатації та технічного обслуговування ІТС кваліфікованого надавача і адміністрування її технічних засобів;

забезпечення функціонування офіційного веб-сайту кваліфікованого надавача;

участь у впровадженні та забезпеченні функціонування КСЗІ або системи управління інформаційною безпекою;

ведення журналів аудиту подій, що реєструє ПТК ІТС кваліфікованого надавача;

встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення ІТС кваліфікованого надавача;

встановлення та налагодження штатної підсистеми резервного копіювання бази даних ІТС кваліфікованого надавача;

забезпечення актуалізації баз даних, створюваних та оброблюваних в ІТС кваліфікованого надавача, у зв'язку із збоями.

4 ПОЛІТИКА СЕРТИФІКАТА

4.1 Перелік сфер, у яких дозволяється використання сертифікатів відкритих ключів, сформованих кваліфікованим надавачем.

4.1.1 Кваліфіковані сертифікати відкритих ключів сформовані кваліфікованим надавачем дозволяється використовувати для:

кваліфікованого електронного підпису;

кваліфікованої електронної печатки;

використання в протоколах узгодження ключа;

ідентифікації особи чи засобу;

аутентифікації засобу чи даних;

удосконаленого електронного підпису;

кваліфікованої електронної позначки часу.

4.1.2 Сертифікати відкритих ключів сформовані кваліфікованим надавачем дозволяється використовувати для:

автентифікації веб-сайту;

4.2. Обмеження щодо використання кваліфікованих сертифікатів відкритих ключів, сформованих кваліфікованим надавачем

Кваліфікований надавач має право встановлювати сфери, в яких дозволяється використовувати кваліфіковані сертифікати відкритих ключів, та визначати обмеження щодо використання сформованих ним кваліфікованих сертифікатів відкритих ключів.

Обмеження щодо використання сформованих кваліфікованим надавачем кваліфікованих сертифікатів відкритих ключів застосовуються відповідно до норм законодавства України. Для кваліфікованих сертифікатів відкритих ключів, сформованих кваліфікованим надавачем, діють обмеження щодо використання кваліфікованого електронного підпису, установлені Порядком використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затвердженого постановою Кабінету Міністрів України від 19 вересня 2018 року № 749.

Інформація щодо обмеження сфери використання доводиться до заявників та підписувачів.

4.3. Перелік інформації, що розміщується кваліфікованим надавачем на своєму офіційному веб-сайті:

загальні відомості про кваліфікованого надавача;

відомості про ВПР кваліфікованого надавача (найменування місцезнаходження, номери телефонів, графік роботи);

дані про внесення відомостей про кваліфікованого надавача до Довірчого списку;

положення цього Регламенту;

кваліфіковані сертифікати відкритих ключів ЦЗО;

кваліфіковані сертифікати відкритих ключів кваліфікованого надавача;

кваліфіковані сертифікати відкритих ключів серверів кваліфікованого надавача (OCSP, TSP, CMP);

списки відкликаних сертифікатів, сформованих кваліфікованим надавачем;

перелік кваліфікованих електронних довірчих послуг, які надає надавач;

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

інформація щодо умов, пов'язаних з обслуговування та використанням кваліфікованих сертифікатів відкритих ключів підписувачів, зокрема:

відомості про обмеження під час використання кваліфікованих сертифікатів відкритих ключів підписувачами;

зобов'язання та підстави відповідальності стосовно використання кваліфікованих сертифікатів відкритих ключів;

Настанова щодо порядку використання програмного забезпечення ІІТ "Користувач ЦСК-1";

інформація щодо порядку перевірки чинності кваліфікованих сертифікатів відкритих ключів, у тому числі умов перевірки їх статусу;

законодавство в сфері електронних довірчих послуг;

переліки та форми документів, які надаються кваліфікованому надавачу для отримання електронних довірчих послуг.

Інформація, яка публікується на інформаційному ресурсі розміщується на HTTP-серверах у вигляді набору web-сторінок.

Кваліфіковані сертифікати відкритих ключів кваліфікованого надавача, а також списки відкликаних сертифікатів розміщуються у складі web-сторінок на HTTP-сервері та у інформаційному дереві LDAP-каталогу на LDAP-сервері.

Доступ до HTTP-серверу здійснюється:

в мережі “Інтернет” за DNS-ім’ям http://ca.mil.gov.ua;

в інформаційно-телекомунікаційній мережі АСУ ЗС України "Дніпро" – http://172.16.1.48:80.

Доступ до LDAP-сервера здійснюється за протоколом LDAP:

в мережі “Інтернет” за DNS-ім’ям http://ca.mil.gov.ua;

в інформаційно-телекомунікаційній мережі АСУ ЗС України "Дніпро" – http://172.16.1.48:80.

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

Кваліфіковані сертифікати відкритих ключів кваліфікованого надавача та його серверів публікуються одразу після їх формування або отримання від Центрального засвідчувального органу (далі – ЦЗО).

Кваліфіковані сертифікати відкритих ключів підписувачів, які надали згоду на їх публікацію, публікуються одразу після формування.

Кваліфікований надавач формує списки відкликаних сертифікатів у вигляді повного та часткового списків.

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

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

Для забезпечення надання кваліфікованих електронних довірчих послуг в закритих інформаційно-телекомунікаційних системах (що немають прямого доступу до ІСД-Інтернет або автоматизованої системи управління Збройних Сил України "Дніпро") може публікуватися тільки повний список відкликаних сертифікатів.

Публікація кваліфікованих сертифікатів відкритих ключів підписувачів здійснюється автоматично з інтервалом синхронізації п’ятнадцять хвилин.

4.5. Механізми підтвердження володіння підписувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката відкритого ключа.

4.5.1. Підтвердження володіння підписувачем особистим ключем відповідний якому відкритий ключ надається на сертифікацію здійснюється під час надання допомоги підписувачу при генерації ключової пари шляхом перевірки удосконаленого електронного підпису без розкриття особистого ключа заявника:

у кваліфікованого надавача або його ВПР – адміністратором реєстрації;

в установі –позаштатним адміністратором реєстрації.

4.5.2. Під час генерації ключової пари позаштатний адміністратор реєстрації в установі або адміністратор реєстрації у кваліфікованого надавача чи його ВПР ідентифікує особу за її особистої присутності за паспортом

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

4.5.3. Відкриті ключі подаються для формування кваліфікованих сертифікатів відкритих ключів у вигляді самопідписаних запитів відповідного формату. Відкриті ключі, можуть надаватись для сертифікації особисто підписувачем, відповідальною особою, або пересилатися через інформаційні мережі (системи електронного документообігу) з застосуванням кваліфікованого електронного підпису для підтвердження їх цілісності та автентичності.

4.5.4. Допускається ідентифікація фізичної особи кваліфікованим надавачем електронних довірчих послуг за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката.

4.6. Умови встановлення заявника (інформація, що надається заявником під час ідентифікації особи, види документів, на підставі яких встановлюється заявник, вимоги щодо особистої присутності).

4.6.1. Ідентифікація заявника, підписувача, відповідальної особи та адміністратора безпеки веб-сервера, здійснюється адміністратором реєстрації за паспортом громадянина України, або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України.

Процедури встановлення особи-заявника повинні використовувати наявні сервіси перевірки чинності документів та ідентифікаційної інформації про особу. До таких сервісів можуть належати сервіси "Перевірка за базою недійсних документів" (nd.dmsu.gov.ua) та "Єдиний державний реєстр юридичних осіб, фізичних осіб - підприємців та громадських формувань" (usr.minjust.gov.ua).

Ідентифікація фізичних осіб, які особисто звертаються до кваліфікованого надавача для отримання електронних довірчих послуг здійснюється за документами, що підтверджують ідентифікаційні дані фізичних осіб.

Ідентифікація фізичних осіб здійснюється за такими ідентифікаційними даними:

- прізвище, ім’я, по батькові (за наявності);

- реєстраційний номер облікової картки платника податків

Для ідентифікації фізичних осіб використовуються:

оригінали (для ознайомлення) та копії (засвідчені встановленим порядком) документів, що посвідчують особу підписувача та підтверджують її ідентифікаційні дані.

відомості щодо належності особи до установи або його повноваження щодо виконання функцій в інтересах установи.

Верифікація даних ID-картки 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;

шляхом автоматизованого зчитування інформації з використанням апаратних та програмних засобів (зчитувачів), які мають відповідний інтерфейс.

У випадках, коли заявники та підписувачі не мають змоги прибути до кваліфікованого надавача чи його ВПР, ідентифікація проводиться в установі позаштатним адміністратором реєстрації. Який назначається наказом кваліфікованого надавача та підпорядковується йому в частині виконання визначених обов'язків адміністратора реєстрації. Заявники та підписувачі мають право ознайомитися з даним наказом .

Установи отримують від кваліфікованого надавача або його ВПР електронні довірчі послуги за заявками керівників установ, які надсилаються разом з додатками на адресу військової частини А0136.

Додатки до заявки:

копія довідки про внесення установи (юридичної особи) до Єдиного державного реєстру юридичних осіб (далі – ЄДРПОУ), звірена в установленому порядку (одноразово);

витяг з наказу або завірена в установленому порядку копія наказу керівника установи про призначення відповідальної особи за організацію використання кваліфікованих електронних довірчих послуг в установі;

Заявка відпрацьовується одноразово за установу. У разі зміни ідентифікаційних даних установи, які вказані в довідці з ЄДРПОУ до кваліфікованого надавача подається заявка на скасування всіх сертифікатів ключів виданих на цю установу та подається новий пакет документів відповідно до первинної процедури отримання електронних довірчих послуг.

У разі зміни відомостей, що містяться у кваліфікованому сертифікаті електронного підпису підписувача, підписувач/відповідальна особа у триденний строк з дня настання таких змін повідомляє про це кваліфікованого надавача та надає документи, що підтверджують відповідні зміни.

На підставі наданих підписувачем/відповідальною особою документів, що підтверджують зміни відомостей, які містяться у кваліфікованому

сертифікаті електронного підпису підписувача, надавач здійснює скасування сертифікату та формування нового відповідно до пунктів 4.5 – 4.6 Регламенту та його публікацію у разі згоди підписувача.

Кваліфікований надавач надає електронні довірчі послуги на найменування установи, яке зазначене в довідці з ЄДРПОУ. Документи на підставі яких установа отримує електронні довірчі послуги від кваліфікованого надавача оформлюються виключно на найменування відповідно до довідки з ЄДРПОУ.

4.6.2. Інформація, що надається під час реєстрації.

Ідентифікаційні дані за установу:

найменування установи, яке зазначене в довідці з ЄДРПОУ;

посада, військове звання, прізвище ім'я та по батькові керівника установи;

юридична адреса;

телефон.

Обов'язкові ідентифікаційні дані підписувача:

прізвище, ім'я та по батькові;

серію і номер паспорта громадянина України, місце його видачі;

реєстраційний номер облікової картки платника податків (РНОКПП) [1];

відомості щодо належності підписувача до установи або його повноваження щодо виконання функцій в інтересах установи;

згода на обробку персональних даних.

Ідентифікаційні дані щодо надання електронних довірчих послуг для ІТС визначається вимогами КСЗІ в цій системі. Ці Вимоги повинні враховувати технічні можливості кваліфікованого надавача.

4.6.3. У разі позитивної ідентифікації, адміністратор реєстрації виконує дії із занесення відомостей про підписувача до бази даних кваліфікованого надавача.

Адміністратор реєстрації не проводить реєстрацію у разі:

відсутності документів, необхідних для ідентифікації підписувача;

відсутності документів, необхідних для реєстрації;

подання підписувачем/відповідальною особою, документів що мають підчистки, дописки, закреслені слова, інші незастережні виправлення, написи олівцем або мають пошкодження, внаслідок чого та якщо їх текст неможливо прочитати;

---

[1] - у разі, якщо через релігійні переконання посадова особа відмовилась від ідентифікаційного коду, до кваліфікованого надавача подається копія сторінки паспорта з відповідною відміткою.

встановлення невідповідності даних.

У разі не проведення реєстрації, один примірник документів, що були надані, повертаються заявнику із відміткою адміністратора реєстрації про невідповідність, другий примірник документів залишається в кваліфікованого надавача.

4.6.4. Ідентифікація заявника, підписувача здійснюється за його особистої присутності:

у кваліфікованого надавача або його ВПР – адміністратором реєстрації;

в установі –позаштатним адміністратором реєстрації.

4.7 Послуга формування, перевірка та підтвердження чинності сертифіката автентифікації домену установи.

4.7.1. Послуга формування сертифіката автентифікації домену надається для використання в ІТС Міністерсва оборони України та Збройних Сил України за заявками керівників установ, які є володільцями або розпорядниками домену.

4.7.2. За заявками керівників установ до сертифікатів відкритих ключів можуть вноситись додаткові відомості з метою їх використання в ІТС Міністерства оборони України та Збройних Сил України.

4.7.3. Перелік додаткових відомостей, які можуть вноситься до сертифікатів та порядок використання таких сертифікатів в ІТС Міністерсва оборони України та Збройних Сил України визначається директивними документами Збройних Сил України.

4.8. Механізм ідентифікації підписувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований кваліфікованим надавачем.

Ідентифікація підписувачів, що мають чинний сертифікат, сформований кваліфікованим надавачем, здійснюється в кваліфікованого надавача за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката.

4.9. Механізм ідентифікації підписувачів з питань блокування, скасування або поновлення кваліфікованих сертифікатів відкритих ключів.

Ідентифікація під час подання заявок на скасування, блокування та поновлення кваліфікованих сертифікатів відкритих ключів здійснюється у порядку, встановленому пунктами 5.6.1-5.6.3 цього Регламенту.

Пункт 4.10. виключно для кваліфікованого надавача.

4.11. Процедурний контроль (система дисциплінарних стягнень за недотримання найманими працівниками надавача своїх посадових обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації надавача та

документації на КСЗІ або систему управління інформаційною безпекою в межах організації з урахуванням режиму роботи надавача)

За недотримання та неналежне виконання персоналом кваліфікованого надавача своїх посадових обов'язків, вимог нормативно-правових актів у сфері електронних довірчих послуг та вимог внутрішньої організаційно-розпорядчої документації надавача та документації на КСЗІ або систему управління інформаційною безпекою в межах організації з урахуванням режиму роботи надавача накладаються дисциплінарні стягнення відповідно до дисциплінарного статуту Збройних Сил України.

Пункти 4.12., 4.13. виключно для кваліфікованого надавача.

4.14. Процес, порядок та умови генерації пар ключів кваліфікованого надавача, підписувачів

Підпункти 4.14.1., 4.14.2. виключно для кваліфікованого надавача.

4.14.3. Генерація пари ключів заявників, підписувачів здійснюється особисто заявником, підписувачем із використанням засобів кваліфікованого електронного підпису безпосередньо в установі, у кваліфікованого надавача або його ВПР під контролем адміністратора реєстрації.

Особистий ключ підписувача захищається паролем. Підписувач несе особисту відповідальність за забезпечення конфіденційності та цілісності особистого ключа.

Перевірку належності підписувачу особистого ключа відповідний якому відкритий ключ надається на сертифікацію здійснюється під час надання допомоги підписувачу при генерації ключової пари адміністратором реєстрації.

Генерація ключової пари підписувача безпосередньо в установі здійснюється за допомогою засобу кваліфікованого електронного підпису чи печатки та програмного забезпечення ІІТ "Користувач ЦСК-1". Настанова щодо порядку використання програмного забезпечення ІІТ "Користувач ЦСК-1" розміщена на інформаційному ресурсі кваліфікованого надавача.

Електронна взаємодія підписувачів, створювачів електронних печаток, яка потребує відправлення, отримання, використання та постійного зберігання за участю третіх осіб електронних даних, аналоги яких на паперових носіях повинні містити власноручний підпис відповідно до законодавства, а також автентифікація в складових частинах інформаційних систем, в яких здійснюється обробка таких електронних даних та володільцями інформації в яких є органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, повинні здійснюватися з використанням кваліфікованих електронних довірчих послуг.

Посадові особи Міністерства оборони України, Апарату Головнокомандувача Збройних Сил України, Генерального штабу Збройних Сил України, органів військового управління, вищих військових навчальних

закладів, військових частин, установ, організацій Збройних Сил України та інших військових формувань, організацій, що діють в інтересах обороноздатності держави для засвідчення чинності відкритого ключа використовують лише кваліфікований сертифікат відкритого ключа, а для реалізації повноважень, спрямованих на набуття, зміну чи припинення прав та/або обов'язків фізичної або юридичної особи, здійснення інформаційного обміну з іншими юридичними особами, застосовують виключно засоби кваліфікованого електронного підпису чи печатки, які мають вбудовані апаратно-програмні засоби, що забезпечують захист записаних на них даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.

Контроль за порядком генерації пари ключів підписувачів здійснює адміністратор реєстрації.

4.15. Процедури отримання підписувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги її кваліфікованим надавачем.

Після генерації підписувачем пари ключів, особистий ключ залишається у нього а відкритий передається на сертифікацію відповідно до пункту 4.16 Регламенту. Відповідальність за забезпечення конфіденційності та цілісності власного особистого ключа несе сам підписувач,

4.16. Механізм надання відкритого ключа підписувача кваліфікованому надавачу для формування сертифіката відкритого ключа

Відкриті ключі на сертифікацію (запити на сертифікацію) подаються до кваліфікованого надавача або його ВПР у вигляді файлів формату PKCS#10:

для формування кваліфікованого сертифіката відкритого ключа особисто підписувачем, відповідальною особою чи позаштатним адміністратором реєстрації,.

для формування сертифіката відкритого ключа особисто адміністратором безпеки веб-серверу чи визначеним представником адміністратора домену (у разі подання відкритого ключа аутентифікації веб-сайту).

Належність запиту на сертифікацію підписувачу підтверджується відповідно пункту 4.5 Регламенту.

При передачі запитів на сертифікацію до кваліфікованого надавача (ВПР) через ІТС, запити на сертифікацію повинні бути засвідчені особистим електронним підписом заявника, підписувача, адміністратора безпеки веб-серверу чи визначеного представника адміністратора домену (у разі подання відкритого ключа аутентифікації веб-сайту).

Пункти 4.17., 4.18. виключно для кваліфікованого надавача.

4.19. Надання електронних довірчих послуг в ІТС де обробляється інформація з обмеженим доступом.

Особливості надання кваліфікованим надавачем електронних довірчих послуг та їх застосування в ІТС де обробляється інформація з обмеженим доступом та системах спеціального зв'язку визначається інструкціями зі складу документації КСЗІ ІТС кваліфікованого надавача та КСЗІ цих систем, а також іншими нормативними документами.

5. ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК

5.1. Процес подання запиту на формування кваліфікованого сертифіката відкритого ключа (перелік суб'єктів, уповноважених здійснювати запит на формування кваліфікованого сертифіката відкритого ключа, порядок подачі та оброблення такого запиту, строки оброблення запиту на формування кваліфікованого сертифіката відкритого ключа)

5.1.1. Запит на сертифікацію являє собою файл формату PKCS#10, що містить відкритий ключ для формування кваліфікованого сертифіката, який формується під час генерації ключової пари засобами кваліфікованого електронного підпису.

Запит на сертифікацію подається до кваліфікованого надавача відповідно до пункту 4.16 Регламенту.

5.2. Надання сформованого кваліфікованого сертифіката відкритого ключа підписувачу

Надання сформованого кваліфікованого сертифіката відкритого ключа підписувачу здійснюється за його вимогою в один із способів:

шляхом запису файлу із сформованим кваліфікованим сертифікатом відкритого ключа на зареєстрований носій інформації, наданий підписувачем/відповідальною особою;

шляхом публікації сформованого кваліфікованого сертифіката відкритого ключа на електронному інформаційному ресурсі кваліфікованого надавача у разі надання згоди на публікацію до формування сертифіката;

шляхом роздрукування – за письмовим запитом;

шляхом завантаження сертифікатів з глобальної мережі з використанням особистого ключа підписувача за допомогою програмного забезпечення ІІТ "Користувач ЦСК-1". Настанова щодо порядку використання програмного забезпечення ІІТ "Користувач ЦСК-1" розміщена на інформаційному ресурсі кваліфікованого надавача.

Підписувач повинен перевірити свої ідентифікаційні дані, внесені до кваліфікованого сертифікату відкритого ключа. Кваліфікований надавач або ВПР повинен надавати відповідні консультації щодо проведення такої перевірки. Підписувач повинен використовувати особистий ключ тільки після позитивного результату перевірки. Використання підписувачем особистого ключа є фактом визнання ним кваліфікованого сертифіката відкритого ключа.

У разі невідповідності ідентифікаційних даних, внесених кваліфікованим надавачем до кваліфікованого сертифікату відкритого ключа та виявлених підписувачем після отримання сформованого кваліфікованого сертифікату відкритого ключа, підписувач звертається до кваліфікованого надавача щодо скасування кваліфікованого сертифіката відкритого ключа. Формування нового особистого ключа та його сертифікація здійснюється у порядку, встановленому цим Регламентом.

5.3. Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа підписувача на офіційному веб-сайті надавача

Сформований кваліфікованим надавачем або ВПР кваліфікований сертифікат відкритого ключа публікуються у відповідності до пункту 4.3 Регламенту.

5.4. Умови використання кваліфікованого сертифіката відкритого ключа підписувача та його особистого ключа (попередження про можливі наслідки неправильного використання кваліфікованого сертифіката відкритого ключа та особистого ключа)

5.4.1. Кваліфікований надавач під час формування кваліфікованого сертифікату відкритого ключа зазначає сфери використання цих сертифікатів та обмеження щодо їхнього використання.

5.4.2. Підписувач використовує особисті та відповідні їм відкриті ключі для накладання та перевірки кваліфікованого електронного підпису чи печатки, зі ступенем розширення основного поля еліптичної кривої не менше 257 згідно з ДСТУ 4145-2002.

5.4.3. Підписувач використовує особисті ключі тільки за призначенням (сферою використання) в період чинності відповідних кваліфікованих сертифікатів відкритих ключів, сформованих відповідно до цього Регламенту, та за умови, що цей сертифікат не був заблокований або скасований а особистий ключ та пароль до нього скомпрометованим.

5.4.4. Перед використанням будь-якого кваліфікованого сертифіката відкритого ключа має забезпечуватись перевірка:

чинності кваліфікованого сертифіката відкритого ключа підписувача, створювача електронної печатки на момент накладення кваліфікованого електронного підпису чи печатки на документ;

чинності кваліфікованого електронного підпису кваліфікованого надавача, що був доданий до кваліфікованого сертифіката відкритого ключа підписувача за допомогою кваліфікованого сертифіката відкритого ключа кваліфікованого надавача, чинного на момент формування кваліфікованого сертифіката відкритого ключа підписувача;

статусу кваліфікованого сертифіката відкритого ключа підписувача у режимі реального часу, якщо перевірка здійснюється на момент чинності цього сертифіката ключа або за списком відкликаних сертифікатів.

5.4.5. Під час перевірки статусу кваліфікованого сертифіката відкритого ключа підписувача за списком відкликаних сертифікатів здійснюється перевірка автентичності, цілісності та терміну дії списку відкликаних сертифікатів.

5.5. Процедура подачі запиту на формування кваліфікованого сертифіката відкритого ключа для підписувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований надавачем

5.5.1. Термін чинності кваліфікованого сертифіката відкритого ключа підписувача становить не більше ніж два роки.

5.5.2. Початок терміну чинності кваліфікованого сертифіката відкритого ключа обчислюється з дати і часу формування сертифіката кваліфікованим надавачем, що відображається у сертифікаті.

5.5.3. Повторне формування кваліфікованого сертифіката відкритого ключа, здійснюється відповідно до первинної процедури формування кваліфікованого сертифікату відкритого ключа, за винятком того, що при повторному зверненні надається тільки картка з реєстраційними даними (якщо дані, які внесені в сертифікат не змінювалися), документ, що підтверджує належність підписувача до установи та надається електронний запит на формування нового кваліфікованого сертифіката відкритого ключа.

5.5.4. Кваліфікований надавач за наявності технічної можливості може повторно сформувати кваліфікований сертифікат відкритого ключа підписувачу чи створювачу електронної печатки, який є власником чинного кваліфікованого сертифіката відкритого ключа, сформованого кваліфікованим надавачем. Формування здійснюється на підставі електронного запиту на формування нового кваліфікованого сертифіката відкритого ключа з накладанням кваліфікованого електронного підпису чи печатки, що відповідає чинному на момент підпису кваліфікованому сертифікату відкритого ключа підписувача чи створювача електронної печатки. Тим самим, кваліфікований електронний підпис чи печатка на зазначеному запиті підтверджують, що ідентифікаційні дані залишаються незмінними.

Ідентифікація підписувача чи створювача здійснюється шляхом перевірки та підтвердження кваліфікованого електронного підпису чи печатки на електронному запиті. Після успішного формування нового кваліфікованого сертифіката відкритого ключа, попередній сертифікат скасовується.

5.6. Обставини скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа; перелік суб'єктів, уповноважених здійснювати запит на скасування (блокування та поновлення) кваліфікованого сертифіката відкритого ключа; процедура подання запиту на скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа; час оброблення запиту на скасування (блокування, поновлення) кваліфікованого сертифіката відкритого ключа; частота формування списку відкликаних сертифікатів та строки його дії; можливість та умови надання інформації про статус кваліфікованого сертифіката відкритого ключа у режимі реального часу)

5.6.1 Скасування кваліфікованого сертифіката відкритого ключа

Скасування кваліфікованого сертифіката відкритого ключа здійснюється у випадках, передбачених частиною першою статті 25 Закону “Про електронні довірчі послуги”.

Скасування кваліфікованого сертифіката відкритого ключа є достроковим припиненням його чинності. Скасовані сертифікати ключів поновленню не підлягають!

5.6.1.1. Скасування кваліфікованого сертифіката відкритого ключа за електронним запитом

Скасування кваліфікованого сертифіката за електронним запитом не потребує оформлення паперових документів.

Дана процедура здійснюється цілодобово за допомогою програмного забезпечення ІІТ "Користувач ЦСК-1" та особистого ключа підписувача.

Процедуру скасування власного кваліфікованого сертифіката відкритого ключа за електронним запитом наведено в Настанові щодо порядку використання програмного забезпечення ІІТ "Користувач ЦСК-1".

Інформування підписувача про скасування здійснюються в режимі реального часу.

5.6.1.2. Скасування кваліфікованого сертифіката відкритого ключа за заявкою у письмовій формі

Письмова заявка на скасування кваліфікованого сертифіката відкритого ключа подається підписувачем або відповідальною особою до кваліфікованого надавача чи його ВПР за встановленою формою, яка публікується на електронному інформаційному ресурсі кваліфікованого надавача.

Кваліфікований надавач або його ВПР встановлює (ідентифікує) особу, яка звертається із заявкою на скасування кваліфікованого сертифіката відкритого ключа, а також перевіряє законність такого звернення.

Обробка такої заявки та інформування клієнта здійснюється протягом двох годин з моменту отримання заявки.

Інформація про зміну статусу кваліфікованого сертифіката відкритого ключа на “скасований” розповсюджується шляхом формування та публікації кваліфікованим надавачем списків відкликаних сертифікатів та за протоколом інтерактивного визначення статусу сертифіката (OCSP).

5.6.2. Блокування кваліфікованого сертифіката відкритого ключа

Блокування кваліфікованого сертифіката відкритого ключа здійснюється у випадках, передбачених частиною шостою статті 25 Закону “Про електронні довірчі послуги”.

Під блокуванням кваліфікованого сертифіката відкритого ключа розуміється тимчасове призупинення чинності кваліфікованого сертифіката строком до 30 календарних днів.

Після блокування кваліфікованого сертифіката відкритого ключа, підписувач може протягом 30 календарних днів поновити строк чинності кваліфікованого сертифіката відкритого ключа. Блокований кваліфікований сертифікат відкритого ключа буде автоматично скасований кваліфікованим надавачем, якщо протягом зазначеного строку не буде поновлено його чинність.

5.6.2.1. Блокування кваліфікованого сертифіката відкритого ключа за електронним запитом

Блокування кваліфікованого сертифіката за електронним запитом не потребує оформлення паперових документів.

Дана процедура здійснюється цілодобово за допомогою програмного забезпечення ІІТ "Користувач ЦСК-1" та особистого ключа підписувача.

Процедуру блокування власного кваліфікованого сертифіката відкритого ключа за електронним запитом наведено в Настанові щодо порядку використання програмного забезпечення ІІТ "Користувач ЦСК-1".

Інформування підписувача про блокування здійснюються в режимі реального часу.

5.6.2.2. Блокування кваліфікованого сертифіката відкритого ключа за заявкою у письмовій формі

Письмова заявка на блокування кваліфікованого сертифіката відкритого ключа подається підписувачем або відповідальною особою до кваліфікованого надавача чи його ВПР за встановленою формою, яка публікується на електронному інформаційному ресурсі кваліфікованого надавача.

5.6.2.3. Блокування кваліфікованого сертифіката відкритого ключа у телефонному режимі

Заявка в усній формі подається підписувачем до кваліфікованого надавача засобами телефонного зв'язку за номерами +38(044)454-41-06, (62) 2-32-06, при цьому підписувач повинен повідомити адміністратору реєстрації наступну інформацію:

ідентифікаційні дані власника кваліфікованого сертифіката відкритого ключа;

ключову фразу голосової автентифікації.

Кваліфікований надавач встановлює (ідентифікує) особу, яка звертається із заявкою на блокування кваліфікованого сертифіката відкритого ключа, а також перевіряє законність такого звернення.

Обробка такої заявки та інформування клієнта здійснюється протягом двох годин з моменту отримання заявки.

Інформація про зміну статусу кваліфікованого сертифіката на "блокований" розповсюджується шляхом формування та публікації кваліфікованим надавачем списків відкликаних сертифікатів та за протоколом інтерактивного визначення статусу сертифіката (OCSP).

5.6.3. Поновлення кваліфікованого сертифіката відкритого ключа

Поновлення кваліфікованого сертифіката відкритого ключа здійснюється у випадках, передбачених частиною десятою статті 25 Закону "Про електронні довірчі послуги".

Поновлення строку чинності кваліфікованого сертифіката відкритого ключа можливе лише для заблокованих кваліфікованих сертифікатів відкритого ключа, термін блокування яких не скінчився.

Для здійснення поновлення строку чинності кваліфікованого сертифіката відкритого ключа, підписувач або відповідальна особа подає до кваліфікованого надавача або його ВПР, письмову заявку за встановленою формою, яка публікується на електронному інформаційному ресурсі кваліфікованого надавача.

Кваліфікований надавач або його ВПР встановлює (ідентифікує) особу, яка звертається із заявкою на поновлення кваліфікованого сертифіката відкритого ключа, а також перевіряє законність такого звернення.

Обробка такої заявки та інформування клієнта здійснюється протягом двох годин з моменту отримання заявки.

Інформація про зміну статусу кваліфікованого сертифіката на "поновлений" розповсюджується шляхом формування та публікації кваліфікованим надавачем списків відкликаних сертифікатів та за протоколом інтерактивного визначення статусу сертифіката (OCSP).

5.7. Строк закінчення дії кваліфікованого сертифіката відкритого ключа підписувача

Строк чинності кваліфікованих сертифікатів відкритих ключів підписувачів становить не більше ніж два роки.

Дата та час початку та закінчення строку чинності ключа зазначається у кваліфікованому сертифікаті відкритого ключа.

Після закінчення строку чинності кваліфікованого сертифіката відкритого ключа, сертифікат вважається не чинним, а застосування відповідного особистого ключа – недійсним.

Частота формування списку відкликаних сертифікатів та строки його дії наведені в пункті 4.4. Регламенту.

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

6.1. Надання засобів кваліфікованого електронного підпису чи печатки

Для надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем використовуються засоби кваліфікованого електронного підпису, які мають позитивний експертний висновок за результатами їх державної експертизи у сфері криптографічного захисту інформації.

Засоби кваліфікованого електронного підпису надаються кваліфікованим надавачем у вигляді:

окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків, здійснюється шляхом розміщення на офіційному ресурсі кваліфікованого надавача або шляхом передачі цих засобів на носіях інформації безпосередньо підписувачеві/відповідальній особі;

апаратно-програмних або апаратних пристроїв через центри забезпечення у яких установи стоять на забезпеченні.

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

Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження кваліфікованої електронної позначки часу надається підписувачам та створювачам електронних печаток при створенні кваліфікованого електронного підпису чи печатки.

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

- формування кваліфікованої електронної позначки часу;

- передачу кваліфікованої електронної позначки часу підписувачеві 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.

Формування та перевірка кваліфікованої електронної позначки часу здійснюється з використанням засобів кваліфікованого електронного підпису.

Перевірка кваліфікованої електронної позначки часу може проводитися будь-яким підписувачем 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 кваліфікованого надавача;

перевіряє кваліфікований електронний підпис, накладений на кваліфіковану електронну позначку часу за допомогою чинного (на момент формування кваліфікованої електронної позначки часу) кваліфікованого сертифіката відкритого ключа кваліфікованого надавача;

перевіряє відповідність кваліфікованої електронної позначки часу та електронних даних, до яких вона додана.

Кваліфікована електронна позначка часу вважається недійсною у разі:

недотримання вимоги щодо точності часу в ПТК;

використання скасованого або блокованого кваліфікованого сертифіката відкритого ключа кваліфікованого надавача на момент формування кваліфікованої електронної позначки часу.

Порядок синхронізації часу із Всесвітнім координованим часом (UTC) погоджується кваліфікованим надавачем із ЦЗО.

6.3. Кваліфікований надавач встановлює вимоги до процедур з управління ризиками, персоналом, операційною безпекою, інцидентами, доказами та архівами, поводження з персональними даними користувачів, процедур встановлення заявника, ВПР та виїзних адміністраторів реєстрації, опису фізичного середовища.

Керівник кваліфікованого надавача електронних довірчих
послуг "Центр сертифікації ключів Збройних Сил України"
полковник Сергій КАЛЕНІЧЕНКО

ПЕРЕЛІК СКОРОЧЕНЬ

АРМ	–	автоматизоване робоче місце
ВПР	–	віддалений пункт реєстрації
ДСТУ	–	державний стандарт України
ЄДРПОУ	–	Єдиний державний реєстр юридичних осіб
ІТС	–	інформаційно-телекомунікаційна система
КСЗІ	–	комплексна система захисту інформації
ОККД	–	облікова картка ключового документа
ПТК	–	програмно-технічний комплекс Центру сертифікації ключів Збройних Сил
ЦЗО	–	Центральний засвідчувальний орган
HTTP	–	Hypertext Transfer Protocol (протокол передачі гіпертексту)
CMP	–	Certificate Management Protocol (протокол управління обслуговуванням сертифікатів)
GPS	–	Global Positioning System (глобальна система позиціонування)
LDAP	–	Lightweight Directory Access Protocol (протокол доступу до каталогу)
NTP	–	Network Time Protocol (мережний протокол синхронізації часу)
OCSP	–	On-line Certificate Status Protocol (протокол визначення статусу сертифіката)
TSP	–	Time Stamp Protocol (протокол фіксування часу)

ЗАТВЕРДЖУЮ
Головнокомандувач Збройних Сил України
генерал

Валерій ЗАЛУЖНИЙ
“4” липня 2022р.

ЗМІНИ № 1 ДО РЕГЛАМЕНТУ
роботи кваліфікованого надавача електронних довірчих послуг
“Центр сертифікації ключів Збройних Сил України”

ПОГОДЖЕНО
Голова Державної служби спеціального зв’язку та захисту інформації України
бригадний генерал

Юрій ЩИГОЛЬ
“___” _____ 2022 р.

ПОГОДЖЕНО
Начальник Центрального управління охорони державної таємниці та захисту інформації Генерального штабу Збройних Сил України
полковник

Сергій ДУДКО
“___” _____ 2022 р.

Київ 2022

ЗМІСТ

Зміни, які вносяться до Регламенту роботи кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України", наведені нижче.

Зміна № 1

Розділ "5.5.3. Повторне формування кваліфікованого сертифіката відкритого ключа, здійснюється відповідно до первинної процедури формування кваліфікованого сертифікату відкритого ключа, за винятком того, що при повторному зверненні надається тільки картка з реєстраційними даними (якщо дані, які внесені в сертифікат не змінювалися), документ, що підтверджує належність підписувача до установи та надається електронний запит на формування нового кваліфікованого сертифіката відкритого ключа", викласти в наступній редакції:

5.5.3. Повторне формування кваліфікованого сертифіката відкритого ключа, здійснюється відповідно до первинної процедури формування кваліфікованого сертифікату відкритого ключа, за винятком того, що при повторному зверненні надається тільки картка з реєстраційними даними (якщо дані, які внесені в сертифікат не змінювалися), документ, що підтверджує належність підписувача до установи та надається електронний запит на формування нового кваліфікованого сертифіката відкритого ключа

На період дії воєнного стану на території України та протягом місяця з дня його припинення чи скасування формування нового сертифікату раніше засвідченого відкритого ключа для користувачів електронних довірчих послуг може здійснюватися кваліфікованим надавачем електронних довірчих послуг автоматично, без особистої присутності користувача, за 10 дів до закінчення строку дії сертифікату.

При цьому раніше сформований сертифікат скасовується, сукупний строк дії раніше сформованого сертифіката та нового сертифіката не перевищує три роки, а строк дії нового сертифіката користувача електронних довірчих послуг не перевищує строку дії власного кваліфікованого сертифіката відкритого ключа надавача електронних довірчих послуг.

ПОРІВНЯЛЬНА ТАБЛИЦЯ

до Регламенту роботи кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України"

Чинна редакція	Редакція, що пропонується
5.5.3. Повторне формування кваліфікованого сертифіката відкритого ключа, здійснюється відповідно до первинної процедури формування кваліфікованого сертифікату відкритого ключа, за винятком того, що при повторному зверненні надається тільки картка з реєстраційними даними (якщо дані, які внесені в сертифікат не змінювалися), документ, що підтверджує належність підписувача до установи та надається електронний запит на формування нового кваліфікованого сертифіката відкритого ключа.	5.5.3. Повторне формування кваліфікованого сертифіката відкритого ключа, здійснюється відповідно до первинної процедури формування кваліфікованого сертифікату відкритого ключа, за винятком того, що при повторному зверненні надається тільки картка з реєстраційними даними (якщо дані, які внесені в сертифікат не змінювалися), документ, що підтверджує належність підписувача до установи та надається електронний запит на формування нового кваліфікованого сертифіката відкритого ключа. **На період дії воєнного стану на території України та протягом місяця з дня його припинення чи скасування формування нового сертифікату раніше засвідченого відкритого ключа для користувачів електронних довірчих послуг може здійснюватися кваліфікованим надавачем електронних довірчих послуг автоматично, без особистої присутності користувача, за 10 дів до закінчення строку дії сертифікату.** **При цьому раніше сформований сертифікат скасовується, сукупний строк дії раніше сформованого сертифіката та нового сертифіката не перевищує три роки, а строк дії нового сертифіката користувача електронних довірчих послуг не перевищує строку дії власного кваліфікованого сертифіката відкритого ключа надавача електронних довірчих послуг.**

Керівник кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України"
підполковник Віталій КІНЧЕВСЬКИЙ

ЗАТВЕРДЖУЮ
Тимчасово виконуючий обов'язки
Головнокомандувача Збройних Сил України
Генерал-майор

Володимир ГОРБАТЮК
"16" 09 2024 р.

ЗМІНИ №2 ДО РЕГЛАМЕНТУ
роботи кваліфікованого надавача електронних довірчих послуг
"Центр сертифікації ключів Збройних Сил України"

ПОГОДЖЕНО
Міністерством цифрової
трансформації України
від 14.08.2024 за № 1/06-2-13223

ПОГОДЖЕНО
Начальник Центрального управління охорони державної таємниці та захисту інформації Генерального штабу Збройних Сил України
полковник

Сергій ДУДКО
"12" 08 2024 р.

Київ 2024

ЗМІСТ

ЗМІНИ,

які вносяться до Регламенту роботи кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України

По тексту Регламенту:

Закон України "Про електронні довірчі послуги" та відповідні посилання **замінити на** Закон України "Про електронну ідентифікацію та електронні довірчі послуги";

постанову Кабінету Міністрів України від 19.09.2018 року № 749 "Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності" та відповідні посилання **замінити на** постанову Кабінету Міністрів України від 01.08.2023 № 798 "Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності";

постанову Кабінету Міністрів України від 07.11.2018 року № 992 "Про затвердження Вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг" та відповідні посилання **замінити на** постанову Кабінету Міністрів України від 28 червня 2024 р. № 764"Про затвердження Вимог до надавачів послуг електронної ідентифікації та електронних довірчих послуг";

словосполучення "адміністратор безпеки та аудиту", **замінити на** "адміністратор безпеки" в усіх родах та відмінках;

словосполучення "інформаційно-телекомунікаційна система", **замінити на** "інформаційно-комунікаційна система" в усіх родах та відмінках;

абревіатуру "ІТС" **замінити на** "ІКС".

В розділі І абзац "наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації від 14.05.2020 року № 269 "Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів та їхніх віддалених пунктів реєстрації" зареєстрованого в Міністерстві юстиції України 16.07.2020 року № 66/34951" **виключити.**

В пункті 1.1. Регламенту словосполучення "просп. Повітрофлотський" **замінити на** "просп. Повітряних сил".

Перші два абзаци пункту 3.1. Регламенту **викласти в наступній редакції:**

"3.1. Перелік посад, посадові обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг є:

адміністратор реєстрації;

адміністратор сертифікації;

адміністратор безпеки;

аудитор системи;

системний адміністратор.

Перелік посад ВПР, посадові обов'язки яких безпосередньо пов'язані з наданням кваліфікованих електронних довірчих послуг є:

керівник відокремленого пункту реєстрації;

адміністратор реєстрації;

відповідальний за захист інформації;

системний адміністратор;

адміністратор сертифікації (за необхідністю).".

Пункт 3.2.3 Регламенту **викласти в наступній редакції:**

"3.2.3. Адміністратор безпеки відповідає за належне функціонування КСЗІ всіх ІКС що забезпечують роботу кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України".

Основними обов'язками адміністратора безпеки є:

участь у генерації пар ключів кваліфікованого надавача та створенні резервних копій особистих ключів кваліфікованого надавача;

участь у знищенні особистих ключів кваліфікованого надавача, контроль за правильним і своєчасним знищенням адміністраторами їх особистих ключів;

організація розмежування доступу до ресурсів ІКС кваліфікованого надавача;

забезпечення організації та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ або системи управління інформаційною безпекою після збоїв, відмов, аварій ІТС кваліфікованого надавача;

забезпечення режиму доступу до приміщень кваліфікованого надавача, в яких розміщена ІТС кваліфікованого надавача;

ведення журналів обліку адміністратора безпеки, визначених документацією на КСЗІ.

Доповнити Регламент пунктом 3.2.3[1] в наступній редакції:

"3.2.3[1]. Аудитор системи відповідає за проведення перевірок дотримання посадовими особами, які виконують обов'язки пов'язані з наданням кваліфікованих електронних довірчих послуг кваліфікованого надавача та його ВПР положень внутрішньої організаційно-розпорядчої документації кваліфікованого надавача та документації щодо КСЗІ ІКС.

Основними обов'язками аудитора системи є:

контроль за формуванням, обслуговуванням і створенням резервних копій кваліфікованих сертифікатів відкритих ключів кваліфікованого надавача, підписувачів та списків відкликаних сертифікатів;

контроль за зберіганням особистих ключів кваліфікованого надавача та їх резервних копій, особистих ключів адміністраторів;

забезпечення спостереження за функціонуванням КСЗІ (реєстрація подій в ІКС кваліфікованого надавача, моніторинг подій тощо);

проведення перевірок журналів аудиту подій, що реєструють технічні засоби ІТС кваліфікованого надавача.

проведення перевірок відповідності положень внутрішньої організаційно-розпорядчої документації кваліфікованого надавача та документації на КСЗІ або систему управління інформаційною безпекою;

контроль за дотриманням посадовими особами кваліфікованого надавача положень внутрішньої організаційно-розпорядчої документації кваліфікованого надавача та документації щодо КСЗІ;

контроль за веденням баз даних кваліфікованого надавача;

контроль за веденням архіву кваліфікованого надавача."

Перший абзац пункту 4.13 Регламенту **викласти в наступній редакції:**

"4.13. Документована інформація у паперовому та/або електронному вигляді, має зберігатися у порядку, встановленому законодавством про архіви та наказами Міністерства оборони України та Генерального штабу Збройних Сил України.".

Пункт 4.14.3 Регламенту **доповнити абзацом наступного змісту:**

"Після генерації підписувачем чи створювачем електронної печатки пари ключів, особистий ключ залишається у нього а відкритий передається на сертифікацію відповідно до пункту 4.16 Регламенту. Відповідальність за забезпечення конфіденційності та цілісності власного особистого ключа та/або атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа несе сам підписувач (заявник)."

Пункт 4.15 Регламенту **викласти в наступній редакції:**

"4.15. Процедури надання підписувачам права використання засобів кваліфікованого електронного підпису чи печатки, розміщених у кваліфікованого надавача, який здійснює генерацію та/або управління парою ключів від імені підписувача чи створювача електронної печатки.

4.15.1 Генерацію та/або управління парою ключів від імені підписувача або створювача електронної печатки може здійснювати виключно кваліфікований надавач. Для генерації та управління особистими ключами використовуються засоби кваліфікованого електронного підпису чи печатки у вигляді апаратно-програмних засобів, що реалізують зберігання множини особистих ключів (наприклад, мережний криптомодуль).

4.15.2 Отримання користувачем особистого ключа у володіння здійснюється за умови 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.

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 кваліфікованим надавачем. Не допускається формування надавачем кваліфікованих сертифікатів відкритих ключів до моменту фактичного отримання особистого ключа користувачем.

Згенерований особистий ключ підписувача чи створювача електронної печатки захищається за допомогою атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа (пароль, PIN-код, OTP-пароль, одноразовий пароль, протокол парного підпису, біометричні дані володільця особистого ключа).

4.15.3 Під час управління парою ключів підписувача або створювача електронної печатки, може здійснювати резервне копіювання особистого ключа підписувача або створювача електронної печатки з метою його зберігання здійснюється з дотримання таких вимог:

рівень безпеки резервної копії особистого ключа відповідає рівню безпеки оригінального особистого ключа;

кількість резервних копій не перевищує мінімального значення, необхідного для забезпечення безперервності послуги.”.

Командир військової частини А0136
полковник Віталій КІНЧЕВСЬКИЙ