ЗАТВЕРДЖУЮ
Начальник Генерального штабу
Збройних Сил України
генерал-лейтенант
Андрій ГНАТОВ
"29" 01 2026 р.

РЕГЛАМЕНТ РОБОТИ

КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ "ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ ЗБРОЙНИХ СИЛ УКРАЇНИ"

на 135 аркушах

ПОГОДЖЕНО
Міністерство цифрової
трансформації України

"___" _____ 2026 р.

ПОГОДЖЕНО
Начальник Центрального управління
охорони державної таємниці та захисту
інформації Генерального штабу
Збройних Сил України
полковник
Сергій ДУДКО
"19" 01 2026 р.

Київ 2026

ЗМІСТ

ВСТУП

Перелік скорочень

ВПР	Відокремлений пункт реєстрації
ЄДДР	Єдиний державний демографічний реєстр
ЄДРПОУ	Єдиний державний реєстр підприємств та організацій України
ЗКЕП	Засіб кваліфікованого електронного підпису чи печатки
ЗС України	Збройні Сили України
ІКС	Інформаційно-комунікаційна система
КЗІ	Криптографічний захист інформації
КНЕДП	Кваліфікований надавач електронних довірчих послуг
КНЕДП ЗС України	Кваліфікований надавач електронних довірчих послуг “Центр сертифікації ключів Збройних Сил України”
КСЗІ	Комплексна система захисту інформації
ОККД	Облікова картка ключового документа
ОС	Операційна система
ПДФО	Податок на доходи фізичних осіб
ПЗ	Програмне забезпечення
ПТК	Програмно-технічний комплекс
РНОКПП	Реєстраційний номер облікової картки платника податків
УНЗР	Унікальний номер запису в ЄДДР
ЦЗО	Центральний засвідчувальний орган
OCSP	Online Certificate Status Protocol
TSP	Time Stamp Protocol
CMP	Certificate Management Protocol

Терміни та визначення

В цьому Регламенті терміни вживаються у такому значенні:

відповідальна особа – посадова особа (посадові особи) або структурний підрозділ, визначені наказом керівника установи, які виконують функції з організації використання кваліфікованих електронних довірчих послуг та мають повноваження щодо подання документів, необхідних для їх отримання у КНЕДП ЗС України;

доменне ім’я – символьне позначення для адресації вузлів мережі та мережевих ресурсів (вебсайтів, серверів електронної пошти, мережевих серверів тощо) в зручній для людини формі;

заявник – користувач, фізична або посадова особа, яка звернулась у встановленому порядку до КНЕДП ЗС України чи його ВПР з метою отримання кваліфікованих електронних довірчих послуг;

облікова картка ключового документа – це документ встановленого КНЕДП ЗС України зразка, що створюється на кожен ключовий документ (носій із зафіксованими ключовими даними) з особистими ключами КНЕДП ЗС України та його серверів;

особи, відповідальні за криптографічні ключі – представники підрозділу з кіберзахисту (служби захисту інформації), криптографічного

захисту інформації або призначені особи в установі, відповідальні за генерацію, застосування та збереження криптографічних ключів для програмних, апаратних засобів, персоналу, мережевих ресурсів (вебсайту або доменного імені) інформаційних, комунікаційних, інформаційно-комунікаційних систем та/або засобів (систем) криптографічного захисту інформації;

підписувачі – фізичні особи, представники установи (військовослужбовці, державні службовці та працівники), які створюють і застосовують кваліфікований електронний підпис для виконання функцій у межах своїх посадових обов'язків;

позаштатний адміністратор реєстрації – посадова особа (посадові особи) установи (керівник, або визначений представник кадрового органу), що здійснює в установі функцію ідентифікації особи користувача, підтвердження володіння ним особистим ключем і перевірку його повноважень;

посадові особи – це військовослужбовці, державні службовці та працівники установ, які виконують організаційно-розпорядчі або адміністративно-господарські функції в межах своїх службових (посадових) обов'язків;

розпорядник вебсайту (доменного імені, інформаційного ресурсу) – установа, якій надано право управляти (розпоряджатися) вебсайтом (доменним іменем, інформаційним ресурсом);

створювачі електронних печаток – установи (юридичні особи), які створюють електронну печатку;

установа – орган військового управління, військова частина, установа або організація, військовий навчальний заклад, територіальний центр комплектування та соціальної підтримки та всі інші юридичні особи, що відносяться до сфери управління Міністерства оборони України та/або підпорядковані (придані) військовому командуванню Збройних Сил України;

фізичні особи – військовослужбовці, державні службовці та працівники установ, що діють в інтересах обороноздатності держави.

Інші терміни, що вживаються в цьому Регламенті, 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 № 764 "Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг", постанові 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" та інших нормативно-правових актах із питань криптографічного та технічного захисту інформації.

Статус Регламенту

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 – КНЕДП ЗС України) під час надання кваліфікованих електронних довірчих послуг, включаючи політику сертифіката та положення сертифікаційних практик.

Цей Регламент розроблено відповідно до:

- Закону України “Про електронну ідентифікацію та електронні довірчі послуги”;
- 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 № 764 “Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг”;
- постанови Кабінету Міністрів України від 23.07.2024 № 842 “Про затвердження переліку документів та електронних даних, отриманих у зв’язку з наданням електронних довірчих послуг, що підлягають постійному зберіганню, та Порядку передачі обслуговування користувачів електронних довірчих послуг, з якими кваліфікований надавач електронних довірчих послуг, що припиняє діяльність з надання кваліфікованих електронних довірчих послуг, уклав договори про надання кваліфікованих електронних довірчих послуг, до іншого кваліфікованого надавача електронних довірчих послуг”;
- постанови Кабінету Міністрів України від 10.12.2024 № 1408 “Деякі питання зберігання документованої інформації та її передавання до центрального засвідчувального органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг”;
- постанови Кабінету Міністрів України від 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”;
- постанови Кабінету Міністрів України від 04.12.2019 № 1137 “Питання Єдиного державного вебпорталу електронних послуг та Реєстру адміністративних послуг”;
- наказ Міністерства цифрової трансформації України від 28.02.2024 № 33 “Про затвердження Регламенту роботи центрального засвідчувального органу”;
- інших нормативно-правових актів у сфері надання електронних довірчих послуг.

Положення цього Регламенту поширюються на:

- посадових осіб КНЕДП ЗС України;
- посадових осіб ВПР КНЕДП ЗС України;
- користувачів електронних довірчих послуг;
- позаштатних адміністраторів реєстрації та відповідальних осіб установ, що застосовують кваліфіковані електронні довірчі послуги;

Вимоги цього Регламенту та його додатків є обов’язковими до виконання посадовими особами КНЕДП ЗС України, його відокремлених пунктів

реєстрації, позаштатних адміністраторів реєстрації та відповідальних осіб установ, що застосовують кваліфіковані електронні довірчі послуги.

Користувачами кваліфікованих електронних довірчих послуг КНЕДП ЗС України та його ВПР є підписувачі, створювачі електронних печаток та особи, відповідальні за криптографічні ключі.

Дотримання вимог цього Регламенту користувачами електронних довірчих послуг є обов'язковою умовою та підставою для надання кваліфікованих електронних довірчих послуг КНЕДП ЗС України.

Вимоги цього Регламенту засновані на принципах дотримання прав і 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 Регламенту на офіційному вебсайті КНЕДП ЗС України.

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

Внесення змін і доповнень до Регламенту

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

Про внесення змін і доповнень до цього Регламенту КНЕДП ЗС України повідомляє користувачів та інших зацікавлених осіб шляхом розміщення зазначених змін і доповнень на своєму офіційному вебсайті.

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

Усі зміни та доповнення, внесені КНЕДП ЗС України до цього Регламенту у зв'язку зі зміною законодавства, набувають чинності одночасно зі вступом у силу відповідних нормативно-правових актів, але не раніше моменту опублікування змін на офіційному вебсайті КНЕДП ЗС України.

1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО КВАЛІФІКОВАНОГО НАДАВАЧА

Повне найменування юридичної особи:

українською – Генеральний штаб Збройних Сил України;

англійською – The General Staff of the Armed Forces of Ukraine.

Скорочене найменування юридичної особи:

українською – ГШ ЗСУ;

англійською – GS of the AFU.

Повне найменування кваліфікованого надавача:

українською – Кваліфікований надавач електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України";

англійською – Qualified trust service provider "Certification Authority of the Armed Forces of Ukraine".

Скорочене найменування кваліфікованого надавача:
українською – КНЕДП “ЦСК Збройних Сил України”;
англійською – QTSP “CSK of Armed Forces of Ukraine”.
Місцезнаходження: 03168, м. Київ, просп. Повітряних Сил, 6.
Код ЄДРПОУ: 22991050.
Номери телефонів: +38(044)454-41-06, (62)2-32-06, (62)2-34-78 (цілодобово, для керування статусом кваліфікованих сертифікатів відкритих ключів підписувачів).
Адреса офіційного електронного ресурсу: https://ca.mil.gov.ua
Адреса електронної пошти: manager@ca.mil.gov.ua
Функції КНЕДП ЗС України виконує структурний підрозділ військової частини А0136. Юридична адреса військової частини А0136: 03022, м. Київ, вул. Михайла Максимовича, 3.

2. ПЕРЕЛІК КВАЛІФІКОВАНИХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

КНЕДП ЗС України 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;
- формування, перевірка та підтвердження чинності сертифіката автентифікації вебсайту;
- зберігання кваліфікованих електронних підписів, печаток, електронних позначок часу та сертифікатів, пов’язаних із цими послугами.

Кожна послуга, що входить до складу електронних довірчих послуг, може надаватися як окремо, так і в сукупності.
Надання зазначених кваліфікованих електронних довірчих послуг здійснюється КНЕДП ЗС України відповідно до цього Регламенту на безоплатній основі для представників установ, що належать до сфери управління Міністерства оборони України та/або підпорядковані (придані) військовому командуванню Збройних Сил України.

3. ПЕРЕЛІК ПОСАД І ФУНКЦІЇ ПЕРСОНАЛУ КВАЛІФІКОВАНОГО НАДАВАЧА

Персоналом КНЕДП ЗС України є посадові особи, які забезпечують виконання організаційних, адміністративних, технічних і технологічних функцій, з метою надання кваліфікованих електронних довірчих послуг, на яких покладено функціональні обов’язки:
- керівника;
- адміністратора реєстрації (віддаленого адміністратора реєстрації);
- адміністратора сертифікації;

- системного адміністратора;
- адміністратора безпеки;
- аудитора системи;
- позаштатного адміністратора реєстрації.

Виконання обов'язків керівника КНЕДП ЗС України покладається на командира військової частини А0136. Виконання обов'язків адміністраторів та аудитора системи покладається на військовослужбовців військової частини А0136 відповідним наказом командира частини.

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

Персонал, що забезпечує роботу ВПР, підпорядковується керівнику КНЕДП ЗС України з питань надання електронних довірчих послуг.

Функції позаштатного адміністратора реєстрації в установі, що звернулась до КНЕДП ЗС України, виконує керівник кадрового органу або визначений представник кадрового органу цієї установи.

КНЕДП ЗС України і його ВПР здійснюють свої повноваження в межах розподілу, визначеного Генеральним штабом Збройних Сил України.

Детальний опис обов'язків персоналу КНЕДП ЗС України та його ВПР визначено в пункті 5.3 Політики сертифіката кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України" (додаток 1 до цього Регламенту) (далі – Політики сертифіката КНЕДП ЗС України).

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 кваліфікованим надавачем

Перелік сфер, в яких дозволяється використання кваліфікованих сертифікатів відкритих ключів визначено в пункті 1.4.1 Політики сертифіката КНЕДП ЗС України.

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

Обмеження щодо використання кваліфікованих сертифікатів відкритих ключів визначено в пункті 1.4.2 Політики сертифіката КНЕДП ЗС України.

4.1.3. Перелік інформації, що розміщується кваліфікованим надавачем на офіційному вебсайті

Перелік інформації, доступ до якої забезпечує КНЕДП ЗС України через офіційний вебсайт зазначено в пункті 2.2 Політики сертифіката КНЕДП ЗС України.

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 КНЕДП ЗС України.

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 КНЕДП ЗС України.

4.1.6. Умови встановлення заявника

Умови встановлення заявника (ідентифікація особи) визначено в пункті 3.2.2 Політики сертифіката КНЕДП ЗС України.

Умови підтвердження повноважень визначено в пункті 3.2.4 Політики сертифіката КНЕДП ЗС України та пункті 3.2.4 Положень сертифікаційних практик кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України" (додаток 2 до цього Регламенту) (далі – Положення сертифікаційних практик КНЕДП ЗС України).

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

Механізм автентифікації користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований КНЕДП ЗС України, визначено в пункті 3.3 Політики сертифіката КНЕДП ЗС України та пункті 3.3 Положень сертифікаційних практик КНЕДП ЗС України.

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

Механізм автентифікації користувачів із питань блокування, скасування або поновлення кваліфікованого сертифіката відкритого ключа визначено в пункті 3.4 Політики сертифіката КНЕДП ЗС України та пункті 3.4 Положень сертифікаційних практик КНЕДП ЗС України.

4.1.9. Опис фізичного середовища

Опис фізичного середовища КНЕДП ЗС України визначено в пункті 5.1 Політики сертифіката КНЕДП ЗС України.

4.1.10. Процедурний контроль

Положення щодо процедурного контролю визначені в пункті 5.2 Політики сертифіката КНЕДП ЗС України.

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 ЗС України, що може здійснювати перегляд журналів аудиту подій, визначено в пункті 5.4 Політики сертифіката КНЕДП ЗС України.

4.1.12. Порядок ведення архівів кваліфікованого надавача

Види документів і даних, що підлягають архівуванню, строки зберігання архівів, механізм і порядок зберігання й захисту архівів і приміщень,

автоматичне резервне копіювання даних, періодичність створення резервних копій і правила збереження з'ємних носіїв визначено в пункті 5.5 Політики сертифіката КНЕДП ЗС України.

4.1.13. Процес, порядок та умови генерації пар ключів кваліфікованого надавача та користувачів

4.1.13.1. Генерація та резервне копіювання особистого ключа кваліфікованого надавача

Процедура генерації особистого ключа КНЕДП ЗС України визначена в пункті 6.1.1.1 Політики сертифіката КНЕДП ЗС України.

Процедура резервного копіювання особистого ключа КНЕДП ЗС України викладена в пункті 6.2.4 Політики сертифіката КНЕДП ЗС України.

4.1.13.2. Генерація та резервне копіювання особистих ключів серверів ІКС кваліфікованого надавача (OCSP, TSP, CMP)

Процедура генерації особистих ключів серверів ІКС КНЕДП ЗС України (OCSP, TSP, CMP) визначена в пункті 6.1.1.1 Політики сертифіката КНЕДП ЗС України.

Процедура резервного копіювання особистих ключів серверів ІКС КНЕДП ЗС України (OCSP, TSP, CMP) викладена в пункті 6.2.4 Політики сертифіката КНЕДП ЗС України.

4.1.13.3. Генерація особистих ключів адміністраторів

Цей пункт Регламенту не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

4.1.13.4. Формування кваліфікованого сертифіката відкритого ключа кваліфікованого надавача

Цей пункт Регламенту не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

4.1.13.5. Формування кваліфікованих сертифікатів відкритих ключів серверів ІКС кваліфікованого надавача (OCSP, TSP, CMP)

Цей пункт Регламенту не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

4.1.13.6. Формування кваліфікованих сертифікатів відкритих ключів адміністраторів

Цей пункт Регламенту не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

4.1.13.7. Використання (введення) особистого ключа кваліфікованого надавача

Процедура використання (введення) особистого ключа КНЕДП ЗС України визначена в пункті 6.2.8 Політики сертифіката КНЕДП ЗС України.

4.1.13.8. Використання (введення) особистих ключів серверів кваліфікованого надавача (OCSP, TSP, CMP)

Процедура використання особистих ключів серверів КНЕДП ЗС України (OCSP, TSP, CMP) визначена в пункті 6.2.8 Політики сертифіката КНЕДП ЗС України.

4.1.13.9. Використання (введення) особистих ключів адміністраторів

Цей пункт Регламенту не входить до обсягу положень, визначених

КНЕДП ЗС України для ознайомлення користувачами.

4.1.13.10. Планова зміна ключів кваліфікованого надавача

Процедура планової зміни ключів КНЕДП ЗС України визначена в пункті 5.6 Політики сертифіката КНЕДП ЗС України.

4.1.13.11. Планова зміна ключів серверів ІКС кваліфікованого надавача (OCSP, TSP, CMP)

Процедура планової зміни ключів серверів ІКС КНЕДП ЗС України (OCSP, TSP, CMP) визначена в пункті 5.6 Політики сертифіката КНЕДП ЗС України.

4.1.13.12. Планова зміна ключів адміністраторів

Цей пункт Регламенту не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

4.1.13.13. Позапланова зміна ключів

Процедура позапланової зміни ключів відповідає процедурі, визначеній у пункті 5.6 Політики сертифіката КНЕДП ЗС України.

Після офіційного оповіщення користувачів про факт позапланової зміни ключів КНЕДП ЗС України забезпечує виконання процедур одержання користувачами нових кваліфікованих сертифікатів відкритих ключів відповідно до вимог цього Регламенту.

4.1.13.14. Процедура ідентифікації користувачем відокремлених пунктів реєстрації кваліфікованого надавача

Ідентифікація ВПР КНЕДП ЗС України здійснюється користувачем відповідно до підпорядкованості військових частин, установ та організацій Збройних Сил України та в межах розподілу, визначеного Генеральним штабом Збройних Сил України. Ідентифікаційні дані ВПР і їхні контактні номери телефонів вказані на інформаційному ресурсі КНЕДП ЗС України.

4.1.13.15. Генерація ключів користувачів

Процедура генерації ключів користувачів визначена в пункті 6.1.1.2 Політики сертифіката КНЕДП ЗС України.

4.1.14. Процедури отримання користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги кваліфікованим надавачем

Процедури отримання користувачем особистого ключа в результаті надання кваліфікованої електронної довірчої послуги КНЕДП ЗС України визначена в пункті 6.1.2 Політики сертифіката КНЕДП ЗС України.

4.1.15. Механізм надання відкритого ключа користувача кваліфікованому надавачу для формування кваліфікованого сертифіката відкритого ключа

Механізм надання відкритого ключа користувача КНЕДП ЗС України для формування кваліфікованого сертифіката відкритого ключа визначено в пункті 6.1.3 Політики сертифіката КНЕДП ЗС України.

4.1.16. Порядок захисту та доступу до особистого ключа кваліфікованого надавача

Цей розділ Регламенту не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

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

Цей розділ Регламенту не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

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 Положень сертифікаційних практик КНЕДП ЗС України.

4.2.2. Порядок надання сформованого кваліфікованого сертифіката відкритого ключа користувачу

Порядок надання сформованого кваліфікованого сертифіката відкритого ключа користувачу визначено в пункті 4.3. Положень сертифікаційних практик КНЕДП ЗС України.

Послідовність дій користувача щодо перевірки даних, що містяться у сформованому кваліфікованому сертифікаті відкритого ключа визначено в пункті 4.4 Положень сертифікаційних практик КНЕДП ЗС України.

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

Порядок публікації сформованого кваліфікованого сертифіката відкритого ключа користувача на офіційному вебсайті КНЕДП ЗС України визначено в пункті 2.2.1 Положень сертифікаційних практик КНЕДП ЗС України.

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 КНЕДП ЗС України.

Кваліфіковані сертифікати відкритого ключа підписувачів і створювачів електронної печатки використовуються у сферах і з обмеженнями, зазначеними в пунктах 1.4.1 та 1.4.2 Політики сертифіката КНЕДП ЗС України.

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.

Підписавши картку з реєстраційними даними (заявку) на отримання кваліфікованих сертифікатів відкритих ключів посадової особи (за формою, розміщеною на інформаційному ресурсі КНЕДП ЗС України), підписувач погоджується з умовами використання кваліфікованого сертифіката відкритого ключа та його особистого ключа.

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

Порядок подачі запиту на формування кваліфікованого сертифіката відкритого ключа для користувачів, які мають чинний кваліфікований сертифікат відкритого ключа, сформований КНЕДП ЗС України, визначено в пункті 4.7 Положень сертифікаційних практик КНЕДП ЗС України.

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 Положень сертифікаційних практик КНЕДП ЗС України.

Порядок блокування та скасування кваліфікованого сертифіката відкритого ключа визначено в пункті 4.9 Положень сертифікаційних практик КНЕДП ЗС України.

Порядок формування списків відкликаних сертифікатів, публікація та розповсюдження списків відкликаних сертифікатів визначено в пункті 2.3 Положень сертифікаційних практик КНЕДП ЗС України.

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 КНЕДП ЗС України.

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

Дата та час початку та закінчення строку дії кваліфікованого сертифіката відкритого ключа користувача зазначається у сертифікаті з 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

Вимоги до процедур з управління ризиками, персоналом, операційною безпекою, інцидентами, доказами та архівами, поводження з персональними даними користувачів, процедур встановлення заявника та ВПР визначаються цим Регламентом, його додатками та організаційно-розпорядчою документацією КНЕДП ЗС України.

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 ЗС України використовуються ЗКЕП, які мають позитивний експертний

висновок за результатами їх державної експертизи у сфері криптографічного захисту інформації.

ЗКЕП надаються КНЕДП ЗС України у вигляді окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків, поширення яких здійснюється шляхом розміщення на офіційному вебсайті КНЕДП ЗС України або на офіційному ресурсі Переліку комп'ютерних програм, які дозволено використовувати в ЗС України.

Апаратно-програмні або апаратні ЗКЕП установи отримують через служби забезпечення інформаційно-комунікаційних систем, у яких ці засоби застосовуються, або організовують закупівлю ЗКЕП за рахунок коштів, які надійшли у вигляді субвенцій і надходжень від повернення 10 % сплаченого ПДФО за військовослужбовців.

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 6.8 Політики сертифіката КНЕДП ЗС України.

6. СХЕМА ЕЛЕКТРОННОЇ ІДЕНТИФІКАЦІЇ

6.1. Перелік схем електронної ідентифікації

Схема електронної ідентифікації включається до переліку схем електронної ідентифікації рішенням Міністерства цифрової трансформації України відповідно до Порядку ведення переліку схем електронної ідентифікації, гаманців з цифровою ідентифікацією, затвердженого постановою Кабінету Міністрів України від 27 лютого 2024 року № 218.

6.2 Встановлення особи та підтвердження ідентифікаційних даних

КНЕДП ЗС України може ідентифікувати особу за ідентифікаційними даними, що містяться в раніше сформованому КНЕДП ЗС України чи іншому КНЕДП кваліфікованому сертифікаті, за умов чинності такого сертифіката та незмінності його ідентифікаційних даних на момент завершення строку дії кваліфікованого сертифікату.

6.3 Поновлення та заміна ідентифікаційних даних

Процедури заміни ідентифікаційних даних передбачають отримання сертифіката. Процедури поновлення даних не передбачені та не виконуються. Допускається ідентифікація особи за ідентифікаційними даними, що містяться в раніше сформованому КНЕДП ЗС України чи іншому КНЕДП кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката

6.4 Процедура ідентифікації власника смарт-підпису

Цей пункт Регламенту не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

Командир військової частини А0136
полковник Віталій КІНЧЕВСЬКИЙ

Додаток 1
до Регламенту роботи кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України"

ПОЛІТИКА СЕРТИФІКАТА КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ "ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ ЗБРОЙНИХ СИЛ УКРАЇНИ"

Київ 2026

ЗМІСТ

1. ВСТУП

1.1.Огляд

Ця Політика сертифіката кваліфікованого надавача електронних довірчих послуг “Центр сертифікації ключів Збройних Сил України” (далі – Політика сертифіката) визначає перелік усіх правил, що застосовуються кваліфікованим надавачем електронних довірчих послуг “Центр сертифікації ключів Збройних Сил України” (далі – КНЕДП ЗС України)і його відокремленими пунктами реєстрації (далі – ВПР) у процесі реєстрації користувачів електронних довірчих послуг, зокрема, підписувачів і створювачів електронних печаток (далі – користувачі), які отримують кваліфіковані електронні довірчі послуги формування та обслуговування кваліфікованих сертифікатів відкритих ключів (далі – кваліфіковані сертифікати) КНЕДП ЗС України та користувачів, а також управління їхнім статусом (блокування, поновлення та скасування).

Дотримання вимог, визначених у цій Політиці сертифіката, є обов’язковим для керівника КНЕДП ЗС України, посадових осіб КНЕДП ЗС України та його ВПР, обов’язки яких безпосередньо пов’язані з реєстрацією користувачів, формуванням й обслуговуванням їхніх кваліфікованих сертифікатів (далі – персонал).

Дотримання користувачами (відповідальними особами) вимог, визначених у цій Політиці сертифіката, є обов’язковою умовою для надання електронних довірчих послуг.

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 “Центр сертифікації ключів Збройних Сил України”.

Скорочена назва документа: Політика сертифіката КНЕДП ЗС України”.

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),	ua	804
Ознака інфраструктури відкритих ключів	root; security; cryptography; ua- pki	2.1.1.1
Ознака політики сертифікації	cp	2

Кваліфіковані сертифікати, сформовані КНЕДП ЗС України, містять об’єктний ідентифікатор (OID) цієї Політики сертифіката, який використовується суб’єктами, які довіряють КНЕДП ЗС України, для визначення придатності та надійності таких сертифікатів під час автентифікації користувачів, зокрема шляхом перевірки та підтвердження електронного підпису чи печатки, а також технічних і програмних засобів шляхом перевірки та підтвердження чинності кваліфікованих сертифікатів.

1.3. Учасники інфраструктури відкритих ключів

До учасників інфраструктури відкритих ключів зазначених у 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. Кваліфікований надавач

КНЕДП ЗС України є кваліфікованим надавачем електронних довірчих послуг, що надає кваліфіковані електронні довірчі послуги з дотриманням вимог Закону України “Про електронну ідентифікацію та електронні довірчі послуги” (далі – Закон), зокрема здійснює реєстрацію користувачів, формування та обслуговування їхніх кваліфікованих сертифікатів, у тому числі управління їхнім статусом (блокування, поновлення та скасування).

КНЕДП ЗС України здійснює реєстрацію користувачів самостійно та/або через ВПР КНЕДП ЗС України.

Відповідні Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг “Центр сертифікації ключів Збройних Сил України” щодо кваліфікованих сертифікатів електронного підпису та печатки (додаток 2 до Регламенту роботи КНЕДП ЗС України) (далі – Положення сертифікаційних практик КНЕДП ЗС України) містять додаткову інформацію.

1.3.1.1. Права кваліфікованого надавача

КНЕДП ЗС України 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 яких міститимуться у кваліфікованому сертифікаті;
- здійснювати під час формування та видачі кваліфікованих сертифікатів перевірку відомостей про осіб, яким видаються такі сертифікати, із використанням інформації з ресурсів Міністерства внутрішніх справ, зокрема даних і відомостей про викрадені або втрачені документи за зверненнями громадян, Єдиного державного реєстру (далі – ЄДР), а також відомостей Державної міграційної служби;
- отримувати консультації від центрального засвідчувального органу (далі – ЦЗО), контролюючого органу (далі – КО) з питань, пов’язаних із наданням електронних довірчих послуг;
- звертатися до органів з оцінки відповідності (далі – 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 із переліку стандартів, визначеного Кабінетом Міністрів України.

1.3.1.2. Обов’язки кваліфікованого надавача

КНЕДП ЗС України зобов’язаний забезпечувати:

- захист персональних даних користувачів відповідно до вимог Закону України “Про захист персональних даних”;
- функціонування ІКС і 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 вебсайту;
- упровадження, підтримання в актуальному стані та публікацію на своєму вебсайті відомостей із реєстру чинних, блокованих і скасованих сертифікатів відкритих ключів;
- можливість цілодобового доступу до реєстру чинних, блокованих і скасованих сертифікатів відкритих ключів і до інформації про статус кваліфікованих сертифікатів через комунікаційні мережі загального користування;

- цілодобовий прийом і перевірку заявок в електронній формі від користувачів (відповідальних осіб) про скасування, блокування та поновлення їхніх кваліфікованих сертифікатів;

- -прийом і перевірку заявок у паперовій формі від користувачів (відповідальних осіб) про скасування, блокування та поновлення їхніх кваліфікованих сертифікатів протягом одного робочого дня після надходження заявки та відповідно до режиму роботи КНЕДП ЗС України;

- скасування, блокування та поновлення кваліфікованих сертифікатів відповідно до вимог Закону;

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

- внесення даних користувача, технічних і програмних засобів до відповідного кваліфікованого сертифіката;

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

- інформування КО та, за 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 із 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 із 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 ЗС України в межах надання послуги створення, перевірки та підтвердження електронного підпису чи електронної печатки;

- постійне зберігання всіх виданих кваліфікованих сертифікатів;

- зберігання документів та електронних даних, отриманих у зв’язку з наданням електронних довірчих послуг у терміни, встановлені чинним законодавством України;

- страхування цивільно-правової відповідальності для забезпечення відшкодування такої шкоди в розмірі, визначеному Законом;

- відновлення розміру страхової суми, яка визначена Законом, протягом трьох місяців у разі зміни розміру мінімальної заробітної плати або в разі відшкодування збитків, завданих користувачам чи третім особам унаслідок неналежного виконання своїх зобов’язань;

- використання під час надання кваліфікованих електронних довірчих послуг виключно кваліфікованих сертифікатів, сформованих ЦЗО;

- залучення військовослужбовців, державних службовців, працівників,

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;

- інформування КО та ЦЗО про намір припинити свою діяльність і про зміни в наданні кваліфікованих електронних довірчих послуг протягом 48 годин із 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 і виконання інших повноважень.

1.3.2. Органи реєстрації

Відокремлені пункти реєстрації КНЕДП ЗС України є органами реєстрації, що представлені окремими підрозділами КНЕДП ЗС України.

До посадових осіб відокремлених пунктів реєстрації КНЕДП ЗС України, на яких покладено обов'язки з реєстрації користувачів, застосовуються такі ж вимоги, як і до адміністраторів реєстрації, що визначені в пункті 5.3.1.2 цієї Політики сертифіката.

Відповідні Положення сертифікаційних практик КНЕДП ЗС України містять додаткову інформацію.

1.3.3. Користувачі

Користувачами кваліфікованих електронних довірчих послуг КНЕДП ЗС України та його ВПР у відповідності до вимог Закону та інших нормативних-правових актів у сферах електронної ідентифікації, електронних довірчих послуг і захисту інформації є: підписувачі, створювачі електронних печаток та особи, відповідальні за криптографічні ключі.

1.3.3.1. Права користувачів

Користувачі мають право на:

- отримання кваліфікованих електронних довірчих послуг;

- оскарження дій чи бездіяльності КНЕДП ЗС України та органів, що здійснюють державне регулювання у сфері електронних довірчих послуг;

- відшкодування завданої їм шкоди та захист своїх прав і законних інтересів;

- звернення із заявкою про скасування, блокування та поновлення особистих кваліфікованих сертифікатів або сертифікатів засобу, персоналу, мережевого ресурсу (вебсайту або доменного імені) ІКС та/або засобу (системи) КЗІ, за які він відповідає.

1.3.3.2. Обов'язки користувачів

Користувачі зобов'язані:

- забезпечувати конфіденційність і неможливість доступу інших осіб до особистого ключа;

- невідкладно повідомляти КНЕДП ЗС України про підозру або факт компрометації особистого ключа;
- надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;
- своєчасно надавати КНЕДП ЗС України 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 кваліфікованому надавачу

Фізичні та юридичні особи, а також їхні ІКС є суб'єктами, які довіряють КНЕДП ЗС України, 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 ЗС України та користувачів, є іншими учасниками.

До інших учасників належать також ЦЗО та КО.

До повноважень ЦЗО, зокрема, належить:

- включення схеми електронної ідентифікації КНЕДП ЗС України до переліку схем електронної ідентифікації;
- погодження плану припинення діяльності КНЕДП ЗС України;
- погодження порядків синхронізації часу із Всесвітнім координованим часом (UTC) КНЕДП ЗС України;
- погодження Регламенту роботи КНЕДП ЗС України.

Адміністратор ІКС ЦЗО, зокрема, забезпечує виконання таких функцій:

- формування кваліфікованих сертифікатів для кваліфікованих електронних довірчих послуг, що надаються КНЕДП ЗС України;
- скасування, блокування та поновлення кваліфікованих сертифікатів КНЕДП ЗС України у випадках, передбачених Законом;
- надання послуг постачання передачі сигналів точного часу, синхронізованого з Державним еталоном одиниць часу і частоти;
- ведення Довірчого списку, зокрема, внесення відомостей про КНЕДП ЗС України до Довірчого списку.

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 ЗС України;
- інформує громадськість у разі отримання від КНЕДП ЗС України

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 ЗС України у рамках позапланових 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 ЗС України формує кваліфіковані сертифікати таких видів:

- кваліфікований сертифікат електронного підпису, що пов’язує відкритий ключ кваліфікованого електронного підпису з фізичною особою або технічним засобом (складовою ІКС, засобом КЗІ тощо) та підтверджує їх ідентифікаційні дані під час створення, перевірки та підтвердження кваліфікованого електронного підпису, а також автентифікації;

- кваліфікований сертифікат електронної печатки, що пов’язує відкритий ключ кваліфікованої електронної печатки з установою та підтверджує її ідентифікаційні дані під час створення, перевірки та підтвердження кваліфікованої електронної печатки, а також автентифікації;

- кваліфікований сертифікат шифрування, що пов’язує відкритий ключ кваліфікованого електронного підпису чи печатки з фізичною особою або технічним засобом (складовою ІКС, засобом КЗІ тощо) в установі та забезпечує направлене шифрування під час обміну інформацією;

- кваліфікований сертифікат автентифікації вебсайту, що пов’язує відкритий ключ кваліфікованого електронного підпису з установою, що є володільцем або розпорядником мережевого ресурсу (вебсайтом або доменним іменем) та забезпечує автентифікацію установи власника (розпорядника) вебсайта та шифрування інформації між учасником онлайн-операції та вебсайтом.

1.4.1.2. Строк дії кваліфікованих сертифікатів

Кваліфіковані сертифікати КНЕДП ЗС України формуються ЦЗО зі строком дії не більше 5 років.

Строк дії кваліфікованих сертифікатів КНЕДП ЗС України становить:

1. СМР 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 14888-3:2019 (ISO/IEC 14888-3:2018, IDT);
- алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

2. особистого ключа КНЕДП ЗС України 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 14888-3:2019 (ISO/IEC 14888-3:2018, 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 5 років з параметрами, що відповідають таким вимогам:

- алгоритм електронного підпису ECDSA з довжиною ключа 256 біт, що відповідає ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT);
- алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447).

Кваліфіковані сертифікати користувачів формуються КНЕДП ЗС України зі строком дії до 2-х років.

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

1.4.2. Заборонене використання сертифіката

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

1.4.3. Використання тестових сертифікатів

Формування тестових сертифікатів здійснюється 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

Реквізити Кваліфікованого надавача електронних довірчих послуг “Центр сертифікації ключів Збройних Сил України”:

Код ЄДРПОУ: 22991050;

Місцезнаходження: 03168, м. Київ, просп. Повітряних Сил, 6;

Номери телефонів: +38 (044)454-41-06, (62)2-32-06, (62)2-34-78;

Адреса електронної пошти: manager@ca.mil.gov.ua;

Веб-сайт: https://ca.mil.gov.ua.

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

Ця Політика сертифіката, а також зміни до неї, затверджуються як додаток до Регламенту роботи КНЕДП ЗС України одноосібно начальником Генерального штабу Збройних Сил України.

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 9.13 цієї Політики сертифіката.

1.6. Визначення термінів та перелік скорочень

1.6.1. Визначення термінів

У цій Політиці сертифіката терміни застосовуються у наступних значеннях:

відповідальна особа – посадова особа (посадові особи) або структурний підрозділ, визначені наказом керівника установи, які виконують функції з організації використання кваліфікованих електронних довірчих послуг та мають повноваження щодо подання документів, необхідних для їх отримання у КНЕДП ЗС України;

доменне ім’я – символьне позначення для адресації вузлів мережі та мережевих ресурсів (вебсайтів, серверів електронної пошти, мережевих серверів, тощо) в зручній для людини формі;

заявник – користувач, фізична або посадова особа, яка звернулась у встановленому порядку до КНЕДП ЗС України чи його ВПР з метою отримання кваліфікованих електронних довірчих послуг;

облікова картка ключового документа – це документ встановленого КНЕДП ЗС України зразка, що створюється на кожен ключовий документ (носій із зафіксованими ключовими даними) з особистими ключами КНЕДП ЗС України та його серверів;

особи, відповідальні за криптографічні ключі – представники підрозділу з кіберзахисту (служби захисту інформації), криптографічного захисту інформації або призначені особи в установі, відповідальні за генерацію, застосування та збереження криптографічних ключів для програмних, апаратних засобів, персоналу, мережевих ресурсів (вебсайту або доменного імені) інформаційних, комунікаційних, інформаційно-комунікаційних систем та/або засобів (систем) криптографічного захисту інформації;

підписувачі – фізичні особи, представники установи (військовослужбовці, державні службовці та працівники), які створюють та застосовують кваліфікований електронний підпис для виконання функцій у межах своїх посадових обов’язків;

позаштатний адміністратор реєстрації – посадова особа (посадові

особи) установи (керівник, або визначений представник кадрового органу), що здійснює в установі функцію ідентифікації особи користувача, підтвердження володіння ним особистим ключем і перевірку його повноважень;

посадові особи – це військовослужбовці, державні службовці та працівники установ, які виконують організаційно-розпорядчі або адміністративно-господарські функції в межах своїх службових (посадових) обов'язків;

розпорядник вебсайту (доменного імені, інформаційного ресурсу) – установа, якій надано право управляти (розпоряджатися) вебсайтом (доменним іменем, інформаційним ресурсом);

створювачі електронних печаток – установи (юридичні особи), які створюють електронну печатку;

установа – орган військового управління, військова частина, установа або організація, військовий навчальний заклад, територіальний центр комплектування та соціальної підтримки та всі інші юридичні особи, що відносяться до сфери управління Міністерства оборони України та/або підпорядковані (придані) військовому командуванню Збройних Сил України;

фізичні особи – військовослужбовці, державні службовці та працівники установ, що діють в інтересах обороноздатності держави.

Інші 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 № 764 "Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг", інших нормативно-правових актах у сферах електронних довірчих послуг, криптографічного та технічного захисту інформації, електронних комунікацій.

1.6.2. Перелік скорочень

ВПР	Відокремлений пункт реєстрації
ГВЧ	Генератор випадкових чисел
ДСТУ	Державний стандарт України
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань
ЄДДР	Єдиний державний демографічний реєстр
ІКС	Інформаційно-комунікаційна система
КНЕДП	Кваліфікований надавач електронних довірчих послуг
ЗС України	"Центр сертифікації ключів Збройних Сил України"
КЗІ	Криптографічний захист інформації
ЗКЕП	Засіб кваліфікованого електронного підпису чи печатки
КО	Контролюючий орган
КСЗІ	Комплексна система захисту інформації

НБУ	Національний банк України
ОККД	Облікова картка ключового документа
ООВ	Орган з оцінки відповідності
ОС	Операційна система
ПЗ	Програмне забезпечення
ПТК	Програмно-технічний комплекс
РНОКПП	Реєстраційний номер облікової картки платника податків
СПЗ	Спеціальне програмне забезпечення
СПФМ	Суб’єкт первинного фінансового моніторингу
УНЗР	Унікальний номер запису в ЄДДР
ЦЗО	Центральний засвідчувальний орган
DNS	Domain Name System
OCSP	Online Certificate Status Protocol
OID	Object identifier
TSP	Time Stamp Protocol
CMP	Certificate Management Protocol
UPN	User Principal Name

2. ОБОВ’ЯЗКИ ЩОДО ПУБЛІКАЦІЇ ТА ЗБЕРІГАННЯ

До об’єктів, процесів і заходів, зазначених у 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 ЗС України забезпечує:

- створення та функціонування вебсайту КНЕДП ЗС України;
- упровадження, підтримання в актуальному стані та публікацію на вебсайті КНЕДП ЗС України відомостей з реєстру чинних, блокованих і скасованих сертифікатів відкритих ключів;
- можливість цілодобового доступу до реєстру чинних, блокованих і скасованих сертифікатів відкритих ключів і до інформації про статус сертифікатів відкритих ключів через комунікаційні мережі загального користування.

КНЕДП ЗС України також забезпечує інформування користувачів про умови отримання кваліфікованих електронних довірчих послуг шляхом розміщення відповідної інформації на вебсайті КНЕДП ЗС України, крім інформації з обмеженим доступом.

КНЕДП ЗС України через вебсайт КНЕДП ЗС України (https://ca.mil.gov.ua) забезпечує вільний доступ до:

- відомостей про КНЕДП ЗС України;
- даних про внесення відомостей про КНЕДП ЗС України до Довірчого списку;
- Політики сертифіката;
- відповідних Положень сертифікаційних практик КНЕДП ЗС України;
- загальних положень та умов надання кваліфікованих електронних

довірчих послуг користувачам КНЕДП ЗС України;

- кваліфікованих сертифікатів КНЕДП ЗС України;
- переліку кваліфікованих електронних довірчих послуг, які надає КНЕДП ЗС України;
- даних про ЗКЕП, що використовуються під час надання кваліфікованих електронних довірчих послуг КНЕДП ЗС України;
- форм документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;
- відомостей про відокремлені пункти реєстрації КНЕДП ЗС України;
- реєстру чинних, блокованих і 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 ЗС України.

КНЕДП ЗС України забезпечує регулярне оновлення інформації та публікацію кваліфікованих сертифікатів, цієї Політики сертифіката, відповідних Положень сертифікаційних практик КНЕДП ЗС України, списків відкликаних сертифікатів, законодавчих актів та інших нормативних документів щодо надання електронних довірчих послуг на вебсайті КНЕДП ЗС України.

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 і виконання користувачами умов надання кваліфікованих електронних довірчих послуг.

Згода на публікацію кваліфікованого сертифіката надається користувачем під час подання картки з реєстраційними даними (заявки) на формування кваліфікованого сертифіката.

КНЕДП ЗС України може визначати обмеження щодо публікації кваліфікованих сертифікатів користувачів на вебсайті КНЕДП ЗС України.

2.2.2. Публікація сертифікатів кваліфікованого надавача

Кваліфіковані сертифікати КНЕДП ЗС України повинні публікуватися на вебсайті КНЕДП ЗС України одразу після їх отримання від ЦЗО.

Кваліфіковані сертифікати серверів КНЕДП ЗС України публікуються одразу після їх формування КНЕДП ЗС України.

КНЕДП ЗС України забезпечує регулярне оновлення інформації та публікацію кваліфікованих сертифікатів, цієї Політики сертифіката, відповідних Положень сертифікаційних практик КНЕДП ЗС України, списків відкликаних сертифікатів (CRL), законодавчих актів та інших нормативних документів щодо надання електронних довірчих послуг на вебсайті КНЕДП

ЗС України: https://ca.mil.gov.ua.

Відповідні Положення сертифікаційних практик КНЕДП ЗС України містять додаткову інформацію.

2.2.3. Доступ до сертифікатів користувачів

Кваліфікований сертифікат користувача після його формування КНЕДП ЗС України 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.

КНЕДП ЗС України може визначати обмеження щодо доступу до кваліфікованих сертифікатів користувачів на вебсайті КНЕДП ЗС України.

2.2.4. Строк дії сертифіката

Строк дії кваліфікованих сертифікатів користувачів становить не більше двох років. Строк дії кваліфікованих сертифікатів КНЕДП ЗС України визначений в п. 1.4.1.2 цієї Політики сертифіката.

Відповідні Положення сертифікаційних практик КНЕДП ЗС України містять додаткову інформацію.

2.3. Час і періодичність публікації

Кваліфіковані сертифікати серверів КНЕДП ЗС України публікуються одразу після їх формування КНЕДП ЗС України.

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

Відповідні Положення сертифікаційних практик КНЕДП ЗС України містять додаткову інформацію.

2.4.Контроль доступу до репозиторію / вебсайту

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

За захист інформації в репозиторії / на вебсайті та базі даних КНЕДП ЗС України відповідає підрозділ із кіберзахисту (позаштатна служба захисту інформації) ІКС КНЕДП ЗС України, до складу якого в обов'язковому порядку включаються адміністратори безпеки та аудитори системи КНЕДП ЗС України. Персональний склад підрозділу з кіберзахисту (позаштатної СЗІ) визначається наказом власника (розпорядника) ІКС КНЕДП ЗС України (керівника КНЕДП ЗС України). Підрозділ із кіберзахисту (позаштатна СЗІ) керується нормативно-правовими актами України, чинними організаційно-розпорядчими, нормативними документами Міністерства оборони України та ЗС України у сфері захисту інформації.

Доступ до управління репозиторієм / вебсайтом і базою даних КНЕДП ЗС України надано підрозділу з кіберзахисту (позаштатної СЗІ) КНЕДП ЗС України та відповідним адміністраторам КНЕДП ЗС України. Захист інформації на вебсайті, у репозиторії та базі даних КНЕДП ЗС України здійснюється відповідно до нормативно-правових актів України, чинних організаційно-розпорядчих, нормативних документів Міністерства оборони

України та ЗС України у сфері захисту інформації.

3. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

До об’єктів, процесів і заходів, зазначених у 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.

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

Основні позначення, що використовуються в кваліфікованих сертифікатах користувачів, наведені в Таблиці 2.

Таблиця 2. Позначення, що використовуються в кваліфікованих сертифікатах користувачів

Найменування	**Значення**
Common Name (CN)	Прізвище, ім’я та по батькові (за наявності) підписувача, якому належить кваліфікований сертифікат, або унікальна назва електронної печатки, або доменне ім’я вебсайту (адреса вебресурсу), або унікальний ідентифікатор технічного засобу (складової ІКС, засобу КЗІ тощо).
Surname (SN)	Прізвище підписувача, якому належить кваліфікований сертифікат.
Given Name (G)	Ім’я та по батькові (за наявності) підписувача, якому належить кваліфікований сертифікат.
SerialNumber (Serial)	Формат атрибута серійного номера визначається: - для користувачів, що є фізичними особами, – як TINUA (Taxpayer Identification Number Ukraine) та РНОКПП або серією (за наявності) та номером паспорта користувача; - для електронної печатки чи технічного засобу (складової ІКС (мережевого ресурсу), засобу КЗІ тощо) – як унікальний реєстраційний номер користувача, що генерується ПТК КНЕДП ЗС України.
Subject Alternative Name (SAN)	Альтернативні ідентифікатори кваліфікованого сертифіката, що можуть містити (за необхідності): - rfc822Name (e-mail) – поштова адреса;

Найменування	Значення
	- dNSName (FQDN) – DNS-імя; - iPAddress (IPv4/IPv6) – IP-адреса; - uniformResourceIdentifier (URI) – єдиний ідентифікатор ресурсу; - directoryName (DN) – назва каталогу; - otherName – інші OID-визначені імена.
UniqueIdentifier (UID)	Унікальний ідентифікатор користувача, якому належить кваліфікований сертифікат.
Organization (O)	Найменування юридичної особи (установи) для кваліфікованих сертифікатів підписувача, електронної печатки, автентифікації вебсайту та технічних засобів (складової ІКС, засобу КЗІ тощо). Для кваліфікованих сертифікатів фізичних осіб, які не належать до юридичної особи (установи), це поле недоступне.
Organizational Unit (OU)	Назва підрозділу або відділу в організації (за необхідності). Для кваліфікованих сертифікатів фізичних осіб, які не належать до юридичної особи, це поле недоступне.
Title (T)	Функціональне призначення електронної печатки чи технічного засобу (складової ІКС, засобу КЗІ тощо). У крайньому випадку може містити посаду підписувача представника юридичної особи (заповнюється за необхідності).
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 № 471
State or Province (S)	Назва області місцезнаходження або місця реєстрації користувача (заповнюється за необхідності)
Locality (L)	Назва населеного пункту місцезнаходження або місця реєстрації користувача (заповнюється за необхідності)
E-Mail Address (E)	Електронна пошта користувача, якому належить кваліфікований сертифікат (заповнюється за необхідності)

За запитом користувача у кваліфікованих сертифікатах можуть міститися додаткові необов’язкові відомості, а саме:

- Телефон;
- Ім’я (DNS – чи інше);
- UPN-ім’я;
- Ідентифікатор НБУ;
- Код СПФМ;
- УНЗР;

- Код організації;
- Код підрозділу;
- Код користувача.

Відповідні Положення сертифікаційних практик КНЕДП ЗС України містять додаткову інформацію.

3.1.1. Типи позначень сертифіката

Типи позначень (реквізитів, атрибутів) кваліфікованого сертифіката, що відповідають відомостям, які містяться у кваліфікованих сертифікатах, визначені в стандартах щодо профілів сертифікатів відповідно до пункту 7.1 цієї Політики сертифіката.

3.1.2. Позначення (реквізити й атрибути) сертифікатів

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

3.1.3. 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 зі стандартом UTF-8.

3.1.5. Унікальність позначень сертифіката

КНЕДП ЗС України 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

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

3.2.1. Метод підтвердження володіння особистим ключем

Підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката, (атрибутів захисту параметрів особистого ключа) забезпечується:

- візуальним і технічним контролем запису та передачі запиту на формування кваліфікованого сертифіката особисто користувачем під час генерації пари ключів одразу після його ідентифікації та підтвердження повноважень (пункти 3.2.2. та 3.2.4 цієї Політики сертифіката);
- технічним контролем запису та передачі запиту на формування кваліфікованого сертифіката особисто користувачем під час генерації пари ключів одразу після підтвердження повноважень та електронної ідентифікації (пункти 3.2.2 та 3.2.4 цієї Політики сертифіката).

Підтвердження володіння користувачем особистим ключем здійснюється без розкриття особистого ключа.

3.2.2. Ідентифікація особи

Формування та видача кваліфікованого сертифіката без ідентифікації користувача та/або представника установи, дані яких міститимуться у кваліфікованому сертифікаті, не допускається.

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

1) за особистої присутності фізичної 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 (наприклад, 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 рівень довіри, раніше виданого особі чи уповноваженому представнику установи за особистої присутності, та багатофакторної автентифікації;

3) за ідентифікаційними даними особи, що містяться у кваліфікованому сертифікаті електронного підпису чи печатки, за умови чинності такого сертифіката;

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

Під час перевірки юридичної особи (з метою формування кваліфікованого сертифіката електронної печатки) КНЕДП ЗС України зобов’язаний використовувати інформацію про юридичну особу, що міститься в ЄДР та є достатньою для формування та видачі кваліфікованого сертифіката.

У випадках передачі обслуговування кваліфікованих сертифікатів користувачів і документованої інформації, на підставі якої були сформовані зазначені сертифікати, від надавача, який припиняє свою діяльність, до КНЕДП ЗС України процедура ідентифікації цих користувачів проводиться одним зі способів, зазначених у цьому пункті, та відповідно до Закону.

Відповідні Положення сертифікаційних практик КНЕДП ЗС України містять додаткову інформацію.

3.2.3. Неперевірена інформація про користувача

Неперевірена інформація про користувача не допускається.

Відповідні Положення сертифікаційних практик КНЕДП ЗС України містять додаткову інформацію.

3.2.4. Підтвердження повноважень

Відповідальна особа (уповноважений представник установи) або особа, відповідальна за криптографічні ключі, (представник установи) підписує документи, необхідні для формування та видачі кваліфікованого сертифіката

підписувача – представника державної установи, електронної печатки, автентифікації вебсайту або технічного засобу (складової ІКС, засобу КЗІ тощо). КНЕДП ЗС України під час формування та видачі такого кваліфікованого сертифіката здійснює ідентифікацію такої особи (пункт 3.2.2 цієї Політики сертифіката), перевіряє обсяг його повноважень за документом від установи та інформацію, що міститься в ЄДР.

У разі формування кваліфікованого сертифіката підписувача здійснюється ідентифікація (пункт 3.2.2 цієї Політики сертифіката) та перевірка повноважень підписувача від установи шляхом перевірки документів, що засвідчують його повноваження або приналежність до юридичної особи, (наказ про призначення, свідоцтво, довідка про проходження служби тощо) або шляхом перевірки інформації у відповідних ІКС (реєстри, бази даних тощо).

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

До об’єктів, процесів і заходів, зазначених у 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 й автентифікація користувача за раніше сформованим кваліфікованим сертифікатом

Користувач може бути ідентифікований за ідентифікаційними даними, що містяться в раніше сформованому кваліфікованому сертифікаті такого користувача, виданого КНЕДП ЗС України, за умови чинності такого сертифіката та незмінності ідентифікаційних даних користувача на момент звернення для отримання послуг у КНЕДП ЗС України.

Перевірка ідентифікаційних даних і повноважень користувача, який звертається з карткою з реєстраційними даними (заявкою) для формування кваліфікованого сертифіката в електронній формі, здійснюється шляхом автентифікації користувача та підтвердження його повноважень за результатами перевірки відповідних кваліфікованих електронних підписів на документах і встановленням їх чинності на момент їх надання.

Відповідні Положення сертифікаційних практик КНЕДП ЗС України містять додаткову інформацію.

3.3.2. Ідентифікація та автентифікація користувача для повторного формування кваліфікованого сертифіката відкритого ключа в разі завершення строку дії попереднього сертифіката

У разі якщо кваліфікований сертифікат користувача скасовано, для формування нового кваліфікованого сертифіката в КНЕДП ЗС України користувач повинен підтвердити свої повноваження, пройти ідентифікацію й автентифікацію згідно з умовами для первинної ідентифікації й автентифікації користувача.

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

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

та ДСТУ ETSI EN 319 411-2.

Скасування, блокування кваліфікованого сертифіката або поновлення заблокованого сертифіката здійснюється на підставі заявки, поданої особисто користувачем, відповідальною особою (уповноваженим представником установи) або представником уповноваженої установи Міністерства оборони України та/або ЗС України в паперовому або електронному вигляді.

Ідентифікація заявника здійснюється відповідно до пункту 3.2.2 цієї Політики сертифіката.

Паперова заявка має містити власноручний підпис заявника.

Блокування кваліфікованого сертифіката може бути здійснено особисто користувачем або відповідальною особою (уповноваженим представником установи) за телефоном із використанням ключової фрази голосової автентифікації.

Пункт 4.8 цієї Політики сертифіката та відповідні Положення сертифікаційних практик КНЕДП ЗС України містять додаткову інформацію.

4. ВИМОГИ ДО ЖИТТЄВОГО ЦИКЛУ СЕРТИФІКАТА

До об’єктів, процесів і заходів, зазначених у 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 до КНЕДП ЗС України на формування кваліфікованого сертифіката належать користувачі, які постійно або тимчасово працюють (проходять службу) в установах (підрозділах), що відносяться до сфери управління Міністерства оборони України та/або підпорядковані (придані) військовому командуванню Збройних Сил України;

Користувачі інших установ, що діють в інтересах оборони України, можуть подавати запит до КНЕДП ЗС України на формування кваліфікованого сертифіката за рішенням Міністерства оборони України, Головнокомандувача Збройних Сил України або Генерального штабу Збройних Сил України.

Запит на формування кваліфікованого сертифіката приймається в обробку після приймання та реєстрації картки з реєстраційними даними (заявки) на формування кваліфікованого сертифіката, ідентифікації (автентифікації) особи користувача, підтвердження володіння користувачем особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката та підтвердження повноважень.

Відкриті ключі на сертифікацію (запити на сертифікацію) подаються до КНЕДП ЗС України або його ВПР у вигляді файлів формату PKCS#10.

Пункт 4.1. Положення сертифікаційних практик КНЕДП ЗС України містить додаткову інформацію.

4.2.Обробка запиту на сертифікат

До об’єктів, процесів і заходів, зазначених у 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 центрального сервера ІКС КНЕДП ЗС України за участю адміністратора реєстрації, 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 і цілісність даних. Автоматична обробка запитів не виключає процесів установлення (ідентифікації) особи заявника, підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката та підтвердження повноважень.

Під час обробки запиту на формування кваліфікованого сертифіката засобами ІКС КНЕДП ЗС України здійснюється перевірка унікальності відкритого ключа в реєстрі чинних, блокованих і скасованих сертифікатів і забезпечується унікальність серійного номера кваліфікованого сертифіката електронного підпису чи печатки.

Розгляд поданої користувачем картки з реєстраційними даними (заявки) на формування кваліфікованого сертифіката з відповідним пакетом документів та опрацювання запиту на сертифікат здійснюється протягом робочого дня.

Строк автоматичного оброблення запиту на формування кваліфікованого сертифіката становить не більше однієї години.

4.3.Формування та видача сертифіката

Формування кваліфікованого сертифіката здійснюється програмними засобами центрального сервера ІКС КНЕДП ЗС України в такій послідовності:

- реєстрації запитів від адміністраторів реєстрації або користувачів на формування сертифікатів користувачів;
- зберігання запитів на формування сертифікатів, отриманих від користувачів та адміністраторів реєстрації, у базі даних запитів;
- формування сертифікатів відкритих ключів користувачів;
- внесення сформованих сертифікатів у реєстр сертифікатів КНЕДП ЗС України.

Формування кваліфікованого сертифіката здійснюється тільки в разі проходження процесів установлення (ідентифікації) особи користувача (заявника), підтвердження володіння ним особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката, підтвердження повноважень, приймання від користувачів та/або адміністраторів реєстрації запиту на формування сертифіката та його обробки.

Автоматичне формування кваліфікованого сертифіката користувача не виключає виконання зазначених процесів.

Надання сформованого кваліфікованого сертифіката користувачу здійснюється шляхом:

- публікації сформованого кваліфікованого сертифіката на вебсайті КНЕДП ЗС України (за умови надання відповідної згоди користувачем);
- зчитування особистого ключа на персональному комп'ютері користувача через програмне забезпечення користувача КНЕДП ЗС України;

- запису файлу зі сформованим кваліфікованим сертифікатом на зареєстрований носій інформації, наданий підписувачем;
- за запитом через захищену систему електронного документообігу Міністерства оборони України.

4.4.Прийняття сертифіката

До об’єктів, процесів і заходів, зазначених у 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 ЗС України відразу після обробки запиту на сертифікат (за умови надання відповідної згоди користувачем).

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

У разі виявлення користувачем протягом однієї доби невідповідності ідентифікаційних даних, внесених КНЕДП ЗС України до кваліфікованого сертифіката, користувач повинен звернутися до КНЕДП ЗС України для скасування вже сформованого кваліфікованого сертифіката та формування нового сертифіката.

4.5.Використання пари ключів і сертифіката

До об’єктів, процесів і заходів, зазначених у 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 і неможливість доступу інших осіб до особистого ключа;
- невідкладно повідомляти КНЕДП ЗС України 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;
- забезпечувати конфіденційність пароля від особистого ключа (атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа).

Користувач зобов’язаний використовувати кваліфікований сертифікат відповідно до зазначеного в 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:

- Регламенту роботи КНЕДП ЗС України;
- цієї Політики сертифіката;
- Положень сертифікаційних практик КНЕДП ЗС України;
- вимог керівних документів щодо надання та застосування кваліфікованих електронних довірчих послуг в ЗС України;

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

Кваліфіковані сертифікати користувачів, сформовані КНЕДП ЗС України, можуть використовуватися будь-якими суб'єктами, які довіряють КНЕДП ЗС України, 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 ЗС України, 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 у кваліфікованому сертифікаті користувача.

4.6.Поновлення сертифіката

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

КНЕДП ЗС України зобов'язаний забезпечувати, зокрема:

- прийом і перевірку заявок у паперовій та електронній формі користувачів про поновлення їхніх кваліфікованих сертифікатів, які були заблоковані КНЕДП ЗС України, протягом одного робочого дня після надходження заявки та відповідно до режиму роботи КНЕДП ЗС України;
- поновлення кваліфікованих сертифікатів, які були заблоковані КНЕДП ЗС України, відповідно до вимог Закону.

Відповідні Положення сертифікаційних практик КНЕДП ЗС України містить додаткову інформацію.

4.7. Повторне формування сертифіката

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

КНЕДП ЗС України здійснює формування кваліфікованого сертифіката користувача за результатами його ідентифікації, підтвердження володіння ним особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката та підтвердження його повноважень в один із таких способів:

- за особистої присутності фізичної особи чи відповідальної особи (уповноваженого представника юридичної особи) – за результатами перевірки 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;

- віддалено (без особистої присутності особи) з одночасним використанням засобу електронної ідентифікації, що має високий або середній рівень довіри, раніше виданого фізичній особі чи відповідальній особі (уповноваженому представнику юридичної особи) за особистої присутності, та багатофакторної автентифікації;
- за ідентифікаційними даними особи, що містяться у кваліфікованому сертифікаті електронного підпису чи печатки, раніше сформованого та виданого згідно з пунктами 1 або 2 частини другої статті 22 Закону, за умови чинності такого сертифіката.

Відповідні Положення сертифікаційних практик КНЕДП ЗС України містять додаткову інформацію.

4.8.Зміна сертифіката

Внесення змін до кваліфікованого сертифіката не допускається.

Відповідні Положення сертифікаційних практик КНЕДП ЗС України містять додаткову інформацію.

4.8.1. Скасування та блокування сертифіката

До об’єктів, процесів і заходів, зазначених у цьому розділі, застосовуються вимоги, визначені в пункті 6.3.9 ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2.

КНЕДП ЗС України зобов’язаний забезпечувати, зокрема:

- прийом і перевірку заявок у паперовій та електронній формі користувачів про скасування та блокування їхніх кваліфікованих сертифікатів, сформованих КНЕДП ЗС України;
- цілодобовий прийом заявок користувачів за ключовою фразою голосової автентифікації про блокування їхніх кваліфікованих сертифікатів, сформованих КНЕДП ЗС України;
- скасування та блокування кваліфікованих сертифікатів, сформованих КНЕДП ЗС України, відповідно до вимог Закону.

Користувач має право за власним бажанням здійснити блокування або скасування власного кваліфікованого сертифіката шляхом подання відповідного електронного запиту, що має бути підписаний із використанням чинного кваліфікованого сертифіката, статус якого необхідно змінити.

Блокування кваліфікованого сертифіката може здійснюватись КНЕДП ЗС України по телефону після проходженням користувачем (відповідальною особою) процедури голосової автентифікації за ключовою фразою, внесеною до картки з реєстраційними даними (заявки).

У разі підозри або підтвердженого факту компрометації особистих ключів користувача блокування сертифікатів може здійснюватись за поданням представників уповноважених установ Міністерства оборони України та/або ЗС України.

Кваліфікований сертифікат вважається заблокованим із моменту зміни його статусу на “заблокований”.

Кваліфікований сертифікат, статус якого змінено на “заблокований”, у період блокування є нечинним і не використовується.

Під блокуванням кваліфікованого сертифіката розуміється тимчасове призупинення дії 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 ЗС України, якщо протягом зазначеного строку користувач не поновить його чинність.

Кваліфікований сертифікат втрачає чинність із моменту зміни його статусу на “скасований”.

Скасований кваліфікований сертифікат поновленню не підлягає.

КНЕДП ЗС України 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 ЗС України.

Публікація списків відкликаних сертифікатів (CRL) відбувається в автоматичному режимі.

Час зміни статусу кваліфікованих сертифікатів синхронізований зі Всесвітнім координованим часом (UTC) із 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 і містить інформацію про всі відкликані сертифікати, які були сформовані КНЕДП ЗС України.

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 і часом формування поточного часткового списку відкликаних сертифікатів.

Відповідні Положення сертифікаційних практик КНЕДП ЗС України містять додаткову інформацію.

4.9.Служби статусу сертифіката

КНЕДП ЗС України забезпечує доступність інформації про статус сертифіката в реальному часі за допомогою OCSP-сервера та списків відкликаних сертифікатів (CRL), що публікуються на вебсайті КНЕДП ЗС України.

4.10. Закінчення строку дії сертифіката

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

Після настання дати та часу закінчення строку дії сертифіката

користувача, зазначеного в ньому, такий сертифікат вважається скасованим.

4.11. Депонування та повернення ключів

Не застосовується.

5. ОБ'ЄКТ, УПРАВЛІННЯ ТА ОПЕРАЦІЙНИЙ КОНТРОЛЬ

До об'єктів, процесів і заходів, зазначених у цьому розділі, застосовуються вимоги, визначені в пунктах 5, 6.3 і 7.3 ДСТУ ETSI EN 319 401.

5.1. Контроль фізичної безпеки

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.2. Процедурний контроль

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

5.3. Контроль персоналу

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.3.1. Довірені ролі персоналу

До складу організаційної структури КНЕДП ЗС України входять такі посадові особи:

1) керівник;
2) адміністратор реєстрації (віддалений адміністратор реєстрації);
3) адміністратор сертифікації;
4) системний адміністратор;
5) адміністратор безпеки;
6) аудитор системи;
7) позаштатний адміністратор реєстрації.

5.3.1.1. Керівник

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.3.1.2. Адміністратор реєстрації (віддалений адміністратор реєстрації)

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.3.1.3. Адміністратор сертифікації

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.3.1.4. Системний адміністратор

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.3.1.5. Адміністратор безпеки

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.3.1.6. Аудитор системи

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.3.1.7. Позаштатний адміністратор реєстрації

Основні функції позаштатного адміністратора реєстрації:

- ідентифікація підписувачів;
- установлення належності підписувачу відкритого ключа та відповідного йому особистого ключа;
- формування карток із реєстраційними даними (заявок) на формування та заявок про блокування, поновлення та скасування кваліфікованих сертифікатів;
- ведення обліку користувачів.

5.3.2. Вимоги щодо кваліфікації, досвіду та допуску персоналу

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.3.3. Вимоги та процедури навчання персоналу

Керівник КНЕДП ЗС України зобов’язаний забезпечити створення умов для безперервної особистої освіти та постійне підвищення кваліфікації персоналу КНЕДП ЗС України у сферах інформаційних технологій, захисту інформації або кібербезпеки та захисту інформації. Персонал КНЕДП ЗС України повинен не менше ніж один раз на два роки проходити курси підвищення кваліфікації.

5.3.4. Санкції за несанкціоновані дії персоналу

Керівництвом КНЕДП ЗС України визначені дисциплінарні стягнення за недотримання персоналом КНЕДП ЗС України своїх посадових обов’язків, вимог нормативно-правових актів у сфері електронних довірчих послуг і вимог внутрішньої організаційно-розпорядчої документації. У межах КНЕДП ЗС України передбачено дисциплінарні стягнення, адміністративну та кримінальну відповідальність відповідно до чинного законодавства.

5.3.5. Контроль відокремлених пунктів реєстрації

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.3.6. Документація, яка надається персоналу

Організаційно-правовий статус керівника та персоналу КНЕДП ЗС України, їх завдання та функції, права та обов’язки, відповідальність, а також професійні знання, досвід і кваліфікація визначаються в посадових інструкціях. Посадові інструкції повинні містити вимоги інформаційної безпеки та методи її забезпечення. Керівник і персонал КНЕДП ЗС України повинні

бути ознайомлені зі своїми посадовими інструкціями Персонал КНЕДП ЗС України повинен бути поінформований про зміни в організації процесів КНЕДП ЗС України, що стосуються їхніх посадових обов'язків.

5.4. Ведення журналу аудиту подій

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.4.1. Типи записаних подій

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.4.2. Частота обробки журналу аудиту подій

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.4.3 Строки зберігання журналу аудиту подій

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.4.4. Захист журналу аудиту подій

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.4.5. Процедури резервного копіювання журналу аудиту подій

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.4.6. Синхронізація часу

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.5. Архів документів

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.5.1. Види документів і даних, що підлягають архівному зберіганню

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.5.2. Строки зберігання архіву

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.5.3. Захист архіву

Цей пункт Політики сертифіката КНЕДП ЗС України не входить

до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.5.4. Процедури резервного копіювання архіву

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.6. Зміна ключа

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.7. Компрометація й аварійне відновлення

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.7.1. Процедури обробки інцидентів і компрометації

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

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

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.7.3. Процедури відновлення після компрометації ключа

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.7.4. Можливості безперервної роботи після катастрофи

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

5.8. Припинення діяльності кваліфікованого надавача

До об’єктів, процесів і заходів, зазначених у 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 ЗС України проводиться відповідно до затвердженого Плану припинення діяльності з надання кваліфікованих електронних довірчих послуг (далі – План припинення діяльності) з урахуванням вимог Закону.

5.8.1. Підстави припинення діяльності кваліфікованого надавача

КНЕДП ЗС України припиняє свою діяльність із надання кваліфікованих електронних довірчих послуг у разі:

1) прийняття ЦЗО рішення про скасування статусу кваліфікованого надавача;

2) прийняття КНЕДП ЗС України рішення про припинення надання кваліфікованих електронних довірчих послуг, зазначених у Довірчому списку;

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

4) набрання законної сили рішенням суду про скасування статусу кваліфікованого надавача.

Про рішення щодо припинення надання кваліфікованих електронних довірчих послуг КНЕДП ЗС України 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 ЗС України 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 ЗС України 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 ЗС України 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 ЗС України повинно містити дату публікації.

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

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

КНЕДП ЗС України, припиняючи свою діяльність з надання кваліфікованих електронних довірчих послуг, передає іншому кваліфікованому надавачу обслуговування користувачів, яким він надавав кваліфіковані електронні довірчі послуги.

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

У разі припинення надання кваліфікованих довірчих послуг КНЕДП ЗС України зобов'язаний передати іншому кваліфікованому надавачу або ЦЗО документовану інформацію (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 буде здійснена КНЕДП ЗС України 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 ЗС України в день, визначений КНЕДП ЗС України як дата припинення діяльності з надання кваліфікованих електронних довірчих послуг, або в день набрання законної сили рішення відповідного суду.

5.8.2. Повідомлення про припинення діяльності кваліфікованого надавача

Про прийняте рішення щодо припинення надання кваліфікованих електронних довірчих послуг КНЕДП ЗС України зобов'язаний повідомити користувачам, ЦЗО та КО не пізніше п'яти робочих днів із дня прийняття такого рішення.

ЦЗО зобов'язаний оприлюднити інформацію про рішення ЦЗО щодо припинення КНЕДП ЗС України діяльності з надання кваліфікованих електронних довірчих послуг, у тому числі у зв'язку зі 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;
- надсилання до КНЕДП ЗС України 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 ЗС України 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 ЗС України повинно містити дату опублікування.

5.8.3. Дата припинення діяльності кваліфікованого надавача

КНЕДП ЗС України припиняє свою діяльність із 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 ЗС України.

З дня опублікування на своєму офіційному вебсайті ЦЗО повідомлення про припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП ЗС України та до дня припинення діяльності з надання кваліфікованих електронних довірчих послуг КНЕДП ЗС України зобов'язаний надавати електронні довірчі послуги, крім формування нових кваліфікованих сертифікатів. ЦЗО у день, визначений як дата припинення діяльності КНЕДП

ЗС України 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 користувачам ЦЗО може прийняти рішення про внесення змін до Довірчого списку щодо заміни кваліфікованого надавача електронних довірчих послуг шляхом заміни відомостей про КНЕДП ЗС України відомостями про іншого кваліфікованого надавача електронних довірчих послуг, якщо передача відповідних прав та обов'язків здійснюється за спільною згодою таких надавачів, у відповідності до підстав для правонаступництва, визначених законодавством.

5.8.5. Передача документованої інформації

КНЕДП ЗС України 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, 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 року № 842;
- Порядку зберігання документованої інформації та її передавання до центрального засвідчувального органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг, затвердженого постановою Кабінету Міністрів України від 10.12.2024 № 1408;
- підпунктів 6.3.4-10A та 6.3.4-11A ДСТУ ETSI EN 319 411-1 та ДСТУ ETSI EN 319 411-2 відповідно.

5.8.6. План припинення діяльності

КНЕДП ЗС України має розроблений і затверджений План припинення діяльності.

План припинення діяльності визначає умови, яких повинен дотримуватися КНЕДП ЗС України 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.

Керівник КНЕДП ЗС України затверджує План припинення діяльності та за необхідності вносить до нього зміни з метою актуалізації інформації, що в ньому міститься.

6. ТЕХНІЧНІ ЗАХОДИ БЕЗПЕКИ

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

6.1. Генерація та встановлення пари ключів

6.1.1. Генерація пари ключів

6.1.1.1. Генерація пари ключів кваліфікованого надавача

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.1.1.2. Генерація пари ключів користувача

Під час надання кваліфікованої електронної довірчої послуги зі створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток КНЕДП ЗС України забезпечується:

- використання користувачем виключно ЗКЕП та кваліфікованого сертифіката;
- захист обміну інформацією між користувачем і КНЕДП ЗС України 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 зі 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 з використанням спеціалізованого програмного забезпечення;
- за допомогою клієнтського мобільного застосунку для смартпристроїв користувачів КНЕДП ЗС України;
- на робочій станції генерації ключів КНЕДП ЗС України та відокремлених пунктів реєстрації КНЕДП ЗС України.

Особистий ключ у складі пари ключів програмних, апаратних засобів, персоналу, мережевих ресурсів (вебсайту або доменного імені) ІКС та/або засобів (систем) КЗІ має бути згенерований відповідно до Інструкцій щодо порядку генерації ключових даних і поводження з ключовими документами, правил користування засобами КЗІ, інструкцій із захисту інформації у відповідній ІКС. Користувач несе персональну відповідальність за дотримання вимог зазначених документів (інструкцій).

Після генерації підписувачем чи створювачем електронної печатки пари ключів особистий ключ залишається в нього, а відкритий ключ передається на сертифікацію.

Якщо пара ключів була згенерована користувачем поза приміщенням КНЕДП ЗС України чи його ВПР та/або за відсутності відповідного персоналу, ідентифікація такого користувача, перевірка його повноважень, формування та видача йому кваліфікованого сертифіката здійснюється КНЕДП ЗС України після перевірки факту володіння користувачем особистим ключем, який відповідає відкритому ключу, наданому для формування кваліфікованого сертифіката.

Для генерації особистих ключів підписувача або створювача електронної печатки використовуються ЗКЕП у вигляді апаратно-програмних засобів (електронні ключі, токени, мережеві криптомодулі), окремих застосунків або програмних модулів (криптобібліотек), що функціонують у складі інших застосунків і перебувають у власності користувачів або надаються КНЕДП ЗС України. Згенерований особистий ключ підписувача або створювача електронної печатки захищається за допомогою одного або декількох атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа (пароль, PIN-код, біометричні дані володільця особистого ключа).

6.1.2. Доставка особистого ключа користувачу

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

- отримання та використання особистого ключа на правах володіння ЗКЕП, який є носієм особистого ключа;
- отримання та використання особистого ключа на правах повного володіння або доступу до частини ресурсу ЗКЕП, який реалізує зберігання множини особистих ключів кваліфікованого електронного підпису чи печатки (наприклад, мережевий криптомодуль).

Фактичне отримання користувачем особистого ключа відбувається в момент генерації особистого ключа особисто або в 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 ЗС України. Не допускається формування КНЕДП ЗС України кваліфікованих сертифікатів до моменту фактичного отримання особистого ключа користувачем.

Відповідальність за забезпечення конфіденційності та цілісності власного особистого ключа та/або атрибутів захисту від доступу сторонніх осіб до параметрів особистого ключа несе сам користувач.

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 й додаткову інформацію для формування кваліфікованого сертифіката.

Запит формату PKCS#10 формується під час генерації особистого

й відкритого ключів засобами кваліфікованого електронного підпису чи печатки.

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

Кваліфіковані сертифікати КНЕДП ЗС України та центрального засвідчувального органу, публікуються на вебсайті КНЕДП ЗС України.

Контейнер ланцюжків сертифікатів, доступний для завантаження суб'єктами, які довіряють КНЕДП ЗС України, розміщений на вебсайті КНЕДП ЗС України за посиланням: https://ca.mil.gov.ua.

Доступ до актуального кваліфікованого сертифіката КНЕДП ЗС України забезпечено на офіційному вебсайті ЦЗО за посиланням: https://czo.gov.ua/ca-registry-details?type=0&id=117.

6.1.5. Розміри (параметри) ключів

В ІКС КНЕДП ЗС України 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 14888-3:2019 (ISO/IEC 14888-3:2018, IDT);
- алгоритм електронного підпису RSA з розміром ключа 4096 біт, що відповідає стандарту PKCS#1 (IETF RFC 3447) або 2048 біт (тільки для ключів користувачів).

6.1.6. Генерація параметрів відкритого ключа

Під час генерації відкритого ключа використовується апаратна генерація ключів за допомогою генератора випадкових чисел (далі – ГВЧ) ЗКЕП (криптомодуля). У ході генерації здійснюється статистична перевірка випадкових бітових послідовностей з апаратного ГВЧ відповідно до Інструкції щодо порядку генерації ключових даних та поводження з ключовими документами відповідного ЗКЕП (криптомодуля). Ключі генеруються та зберігаються у відповідному ЗКЕП (криптомодулі).

6.1.7. Основні цілі використання особистого ключа кваліфікованим надавачем

Особисті ключі КНЕДП ЗС України забезпечують функціонування ІКС КНЕДП ЗС України.

КНЕДП ЗС України визначає практику використання ключів КНЕДП ЗС України для підпису сертифікатів користувачів, сертифікатів серверів OCSP, СМР КНЕДП ЗС України, 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 КНЕДП ЗС України та серверів ІКС КНЕДП ЗС України використовуються мережеві криптомодулі, що виконані у вигляді окремих апаратних пристроїв. Криптомодулі повинні мати документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами експертизи (сертифікації) таких засобів.

Для зберігання особистих ключів підписувачів КНЕДП ЗС України використовує ЗКЕП, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами експертизи (сертифікації) таких засобів.

Для зберігання особистих ключів програмних, апаратних засобів, персоналу, мережевих ресурсів (вебсайту або доменного імені) ІКС та/або засобів (систем) КЗІ застосовуються носії відповідно до вимог Інструкцій щодо порядку генерації ключових даних та поводження з ключовими документами, правил користування засобами КЗІ, інструкцій із захисту інформації в відповідній ІКС.

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

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.2.3. Управління особистим ключем підписувача

Управління парою ключів від імені підписувача або створювача електронної печатки може здійснювати виключно КНЕДП ЗС України. КНЕДП ЗС України забезпечує зберігання та захист особистих ключів користувачів, згенерованих у мережевих криптомодулях, які мають документальне підтвердження про відповідність вимогам статей 18 і 19 Закону, видане за результатами експертизи (сертифікації) таких засобів, які розміщені в спеціальних серверних приміщеннях, доступ до яких мають тільки відповідальні особи КНЕДП ЗС України.

КНЕДП ЗС України забезпечує обслуговування, зберігання та захист особистих ключів користувачів у мережевих криптомодулях.

6.2.4. Резервне копіювання особистого ключа

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.2.5. Архівація особистого ключа

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.2.6. Відновлення особистого ключа

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.2.7. Зберігання особистого ключа в криптографічному модулі

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.2.8. Активація особистих ключів

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.2.9. Деактивація особистих ключів

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.2.10. Знищення особистих ключів

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.2.11. Можливості мережевого криптографічного модуля

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

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 ЗС України в складі сертифікатів постійно.

Засоби, що входять до складу центрального сервера КНЕДП ЗС України, забезпечують автоматичне резервне копіювання реєстру кваліфікованих сертифікатів. Автоматичне створення резервної копії має виконуватися не рідше 1 разу на добу під час найменшого завантаження центрального сервера.

Додатково може виконуватися резервне копіювання кваліфікованих сертифікатів підписувачів на знімні носії інформації в ручному режимі. Після створення нової резервної копії попередня резервна копія стає архівною.

Відновлення кваліфікованих сертифікатів із резервної копії здійснюється засобами ПТК шляхом зчитування кваліфікованих сертифікатів з останньої (актуальної) резервної копії та їх запису в базу даних сервера.

Архівні копії кваліфікованих сертифікатів КНЕДП ЗС України його серверів й адміністраторів, а також підписувачів мають зберігатися постійно.

6.3.2. Строки дії сертифіката та строки використання пари ключів

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

- для особистих ключів КНЕДП ЗС України та його серверів (OCSP, CMP, TSP) – не більше 5 років;
- для особистих ключів адміністраторів і користувачів – не більше 2 років.

6.4. Дані активації

6.4.1. Створення та встановлення даних активації

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.4.2. Захист даних активації

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.4.3. Інші аспекти даних активації

Жодних інших аспектів.

6.5. Контроль комп'ютерної безпеки

6.5.1. Спеціальні технічні вимоги до комп'ютерної безпеки

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.5.2. Рейтинг комп'ютерної безпеки

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.6. Контроль безпеки життєвого циклу

6.6.1. Контроль розробки системи

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.6.2. Засоби керування безпекою

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.6.3. Контроль безпеки протягом життєвого циклу

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.7. Контроль безпеки мережі

Цей пункт Політики сертифіката КНЕДП ЗС України не входить до обсягу положень, визначених КНЕДП ЗС України для ознайомлення користувачами.

6.8. Електронні 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;
- перевірка та підтвердження кваліфікованої електронної позначки часу.

Кваліфікована електронна позначка часу має презумпцію точності дати та часу, на які вона вказує, цілісності електронних даних, із якими ці дата та час пов'язані та повинна відповідати таким вимогам:

- пов'язувати дату й час з електронними даними в такий спосіб, що обґрунтовано виключає можливість зміни електронних даних, яку неможливо виявити;
- базуватися на джерелі точного часу, синхронізованому зі Всесвітнім координованим часом (UTC) з точністю до секунди.

6.8.1. Формування кваліфікованої електронної позначки часу

Формування кваліфікованої електронної позначки часу здійснюється

КНЕДП ЗС України за запитом користувача.

Під час формування кваліфікованої електронної позначки часу користувач та КНЕДП ЗС України за допомогою ЗКЕП виконують 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 ЗС України;

4) КНЕДП ЗС України перевіряє правильність формату запиту та здійснює його обробку, формує кваліфіковану електронну позначку часу й відповідь, що містить кваліфіковану електронну позначку часу, чи відповідь з інформацією про відмову у формуванні кваліфікованої електронної позначки часу;

5) КНЕДП ЗС України надсилає користувачеві відповідь, що містить кваліфіковану електронну позначку часу, у 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 ЗС України, накладені на кваліфіковану електронну позначку часу;

6) користувач після отримання відповіді від КНЕДП ЗС України виконує 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 ЗС України;
- перевіряє відповідність призначення сертифіката КНЕДП ЗС України (для формування позначки часу);
- перевіряє чинність сертифіката КНЕДП ЗС України;
- перевіряє кваліфікований електронний підпис чи печатку, що були накладені на кваліфіковану електронну позначку часу;
- перевіряє відповідність електронних даних і даних, для яких була сформована кваліфікована електронна позначка часу (шляхом порівняння обчисленого геш-значення електронних даних і геш-значення, записаного у кваліфікованій електронній позначці часу);

- додає кваліфіковану електронну позначку часу до електронних даних.

6.8.2. Перевірка кваліфікованої електронної позначки часу

Перевірка кваліфікованої електронної позначки часу може проводитися будь-якою особою з метою підтвердження кваліфікованої електронної позначки часу.

Під час перевірки та підтвердження кваліфікованої електронної позначки часу особа, що проводить перевірку, виконує такі дії:

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

6.8.3. Недійсність кваліфікованої електронної позначки часу

Кваліфікована електронна позначка часу вважається недійсною в разі:

- недотримання вимоги щодо точності часу в програмно-технічному комплексі КНЕДП ЗС України;
- використання скасованого або блокованого сертифіката КНЕДП ЗС України на момент формування кваліфікованої електронної позначки часу.

Правильність реалізації криптографічних алгоритмів для створення кваліфікованої електронної позначки часу та точність часу в ЗКЕП забезпечує протокол фіксування часу.

6.8.4. Отримання кваліфікованої електронної позначки часу кваліфікованим надавачем

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

Механізм синхронізації часу зі Всесвітнім координованим часом (UTC) в програмно-технічному комплексі КНЕДП ЗС України та склад технічного обладнання, що застосовується у процесі синхронізації часу (його загальний опис) установлюється Порядком синхронізації часу зі Всесвітнім координованим часом (UTC).

Порядок синхронізації часу зі Всесвітнім координованим часом (UTC) розробляється КНЕДП ЗС України та погоджується з ЦЗО.

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

До об’єктів, процесів і заходів, зазначених у цьому розділі, застосовуються вимоги, визначені в пунктах 6.6 ДСТУ ETSI EN 319 411-1

та ДСТУ ETSI EN 319 411-2.

7.1. Профілі сертифікатів

Кваліфіковані сертифікати, що формуються КНЕДП ЗС України 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 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 (v3) 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 кваліфікованого 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)

Найменування	Значення
Відкритий ключ	Відкритий ключ, що відповідає особистому ключу кваліфікованого сертифіката (відповідно до стандарту RFC 5280)
Підпис	Кваліфікований електронний підпис кваліфікованого надавача, що надає послугу створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки згенерований і закодований відповідно до стандарту RFC 5280.

7.2. Профілі списку відкликаних сертифікатів (CRL)

Списки відкликаних сертифікатів (CRL), що формуються КНЕДП ЗС України, 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 ЗС України, відповідає стандарту ITU-T X.509 та регламенту RFC 5280. CRL повинен мати принаймні такі поля:

Найменування	Значення
Версія	Версія CRL (version 2).
Емітент	Назва кваліфікованого 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 гешування підпису	Алгоритм гешування
Підпис	Значення цифрового підпису від кваліфікованого 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 з 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 Й ІНШІ ОЦІНКИ

До об’єктів, процесів і заходів, зазначених у цьому розділі, застосовуються вимоги, визначені в пунктах 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 ЗС України 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 ЗС України перебуває під наглядом КО, функції якого виконує Адміністрація Державної служби спеціального зв’язку та захисту інформації України.

КО у випадках, визначених законодавством, може:

1) здійснити позапланову перевірку дотримання кваліфікованим 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 кваліфікованого 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 кваліфікований надавач повідомляє КО шляхом надання копії документа про відповідність не пізніше трьох робочих днів із дня його отримання.

КНЕДП ЗС України 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 пункті8.2 цієї Політики сертифіката.

КНЕДП ЗС України проходить оцінку відповідності згідно з вимогами:

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

КНЕДП ЗС України проходить щорічне оцінювання (аудит) системи захисту інформації та отримує звіт із проходження оцінювання (аудиту) системи захисту інформації.

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 – Виїзна перевірка) здійснюється посадовими особами КО відповідно до їхніх функціональних обов’язків за адресою знаходження КНЕДП ЗС України.

Виїзна перевірка здійснюється відповідно до рішення КО.

Рішення щодо проведення Виїзної перевірки повинно містити:

- найменування Адміністрації Державної служби спеціального зв’язку та захисту інформації України;
- найменування кваліфікованого надавача;
- місцезнаходження кваліфікованого надавача;
- підставу для проведення перевірки;
- предмет перевірки;
- дати початку та закінчення перевірки;
- посадовий і 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 кваліфікованих надавачів і послуг, що ними надаються.

ООВ повинен мати спеціальний дозвіл на провадження діяльності, пов'язаної з державною таємницею.

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 року № 512.

8.2.3. Вимоги до кваліфікації організації, що проводить оцінювання (аудит) із питань відповідності у сфері захисту інформації

Для здійснення оцінювання дотримання вимог цільового профілю безпеки ІКС КНЕДП ЗС України юридичні особи, фізичні особи – підприємці мають відповідати одній із таких вимог:

1) наявність ліцензії на провадження господарської діяльності з надання послуг у галузі технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України, у частині (залежно від інформації, що обробляється в інформаційній, електронній комунікаційній, інформаційно-комунікаційній, технологічній системі (відкрита інформація чи інформація з обмеженим доступом)):

оцінювання захищеності інформації, що не становить державної таємниці;

оцінювання захищеності інформації всіх видів, у тому числі інформації, що становить державну таємницю;

2) наявність дозволу на проведення робіт технічного захисту інформації для власних потреб у частині (залежно від інформації, що обробляється в інформаційній, електронній комунікаційній, інформаційно-комунікаційній, технологічній системі (відкрита інформація чи інформація з обмеженим доступом)):

оцінювання захищеності інформації, що не становить державної таємниці;

оцінювання захищеності інформації всіх видів, у тому числі інформації, що становить державну таємницю.

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, із якими (або зі службовими особами яких) посадова особа перебуває в родинних стосунках, або в разі виникнення в неї конфлікту інтересів згідно

із законодавством у сфері запобігання та 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 із керівником і персоналом КНЕДП ЗС України;
- ознайомлювати керівника КНЕДП ЗС України чи уповноваженого ним представника з результатами перевірки;
- надавати КНЕДП ЗС України 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 оцінювачів (експертів, аудиторів), що проводять оцінку відповідності, з об'єктом оцінки

Оцінювачі (експерти, аудитори), що проводять оцінку відповідності, повинні бути незалежними та не мати спільних ділових інтересів із КНЕДП ЗС України, що можуть впливати на результати оцінювання. Оцінювачі (експерти, аудитори), що проводять оцінку відповідності, повинні мати допуск до державної таємниці.

8.3.3. Відносини експертів, що проводять оцінювання (аудит) системи захисту інформації

Документами, що регламентують відносини між КНЕДП ЗС України та оцінювачами (експертами, аудиторами), є визначений порядок проведення авторизації з безпеки в ІКС Міністерства оборони України, Збройних Сил України та Державної спеціальної служби транспорту, а також відповідні накази (розпорядження).

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 КНЕДП ЗС України за такими питаннями:

- загальні вимоги;
- забезпечення безпеки інформаційних ресурсів;
- кадрові ресурси;
- експлуатація ЗКЕП;
- вимоги до надання електронних довірчих послуг;
- політика сертифіката;
- положення сертифікаційних практик;
- надання кваліфікованої електронної довірчої послуги зі 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.

8.4.3. Питання, що підлягають перевірці під час оцінювання (аудиту) системи захисту інформації

Перелік питань, які розглядаються в межах оцінювання (аудиту), визначаються у плані проведення оцінювання (аудиту). План проведення оцінювання (аудиту) узгоджується з КНЕДП ЗС України.

8.5. Дії, вжиті внаслідок порушень

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 й 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 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 такі заходи реагування:

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

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

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

Рішення про блокування або скасування кваліфікованого сертифіката КНЕДП ЗС України 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 ЗС України, у Довірчому списку в разі:

- надання кваліфікованих електронних довірчих послуг КНЕДП ЗС України без чинних документів, визначених законодавством,

що підтверджують відповідність заходів та/або системи з безпеки інформації (системи захисту інформації 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 ЗС України поточного рахунку зі спеціальним режимом використання в банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) із необхідним обсягом коштів або чинного договору страхування цивільно-правової відповідальності з необхідним розміром страхової суми, що встановлені Законом, для забезпечення відшкодування збитків, які можуть бути завдані користувачам електронних довірчих послуг або третім особам унаслідок неналежного виконання кваліфікованим надавачем своїх зобов'язань;
- порушення заходів із безпеки (захисту) інформації та/або вимог до умов експлуатації системи з безпеки інформації (системи захисту інформації) ІКС КНЕДП ЗС України;
- надання кваліфікованих електронних довірчих послуг КНЕДП ЗС України 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;
- установлення факту надання недостовірних відомостей, наведених у документах, поданих КНЕДП ЗС України для внесення відомостей про нього до Довірчого списку;
- неусунення виявлених під час перевірки порушень у встановлений приписом строк;
- блокування або скасування кваліфікованого сертифіката КНЕДП ЗС України.

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 приймає 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 вимогам у сфері електронних довірчих послуг ООВ видає замовнику процедури оцінки відповідності аудиторський звіт із висновками про невідповідність і переліком недоліків.

Результати оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг аналізуються КО. У разі негативних результатів оцінки відповідності та/або на підставі 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 кваліфікованого надавача або послуги, яку надає кваліфікований надавач, у Довірчому списку в разі надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем без чинних документів, визначених законодавством, що підтверджують відповідність заходів та/або системи з безпеки інформації (системи захисту інформації ІКС КНЕДП ЗС України 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.

8.5.3. Дії, що вживаються внаслідок порушення, виявленого за результатами оцінювання (аудиту) системи захисту інформації

У разі виявлення невідповідності вимогам оцінювачі (експерти, аудитори) розроблюють план корегувальних дій.

Строк доопрацювання визначається оцінювачами (експертами, аудиторами) спільно з КНЕДП ЗС України.

Після виконання корегувальних дій може проводитись додаткова перевірка з оцінкою усунення недоліків.

8.6. Повідомлення результатів

8.6.1. Оформлення результатів державного контролю

Результати проведення перевірки кваліфікованого надавача оформлюються комісією з перевірки шляхом складання акта перевірки, форма якого затверджується КО.

Акт перевірки має містити такі відомості:

- найменування КО;
- персональний і посадовий склад комісії з перевірки;
- прізвище та ініціали керівника кваліфікованого надавача;
- реквізити посвідчення на проведення перевірки;
- дати початку та закінчення перевірки;
- адреси приміщень кваліфікованого надавача, у 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 кваліфікованого надавача, пов’язану з наданням електронних довірчих послуг;
- виявлені під час перевірки порушення й недоліки (за наявності) та пояснення кваліфікованого 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 складання акта перевірки;
- підписи голови та членів комісії з перевірки;
- підпис керівника кваліфікованого надавача чи уповноваженого ним представника, що підтверджує факт ознайомлення з актом перевірки.

Акт перевірки складається у двох примірниках і підписується не пізніше останнього дня її проведення головою та всіма членами комісії з перевірки та керівником кваліфікованого 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 кваліфікованого надавача чи уповноважений ним представник має зауваження щодо фактів і висновків, викладених в акті перевірки, перед підписом зазначається "Із зауваженнями, що додаються".

Зауваження до акта перевірки оформлюються окремим документом і підписуються керівником кваліфікованого надавача чи уповноваженим ним представником.

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

Якщо керівник кваліфікованого 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 кваліфікованого надавача чи уповноваженого ним представника робить відповідний запис, який 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 в 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 із дня складання акта перевірки надається кваліфікованому надавачу, а другий примірник із підписом керівника кваліфікованого 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 кваліфікованого 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 кваліфікованого надавача повинен вжити заходи до усунення недоліків і порушень, зазначених у приписі про усунення порушень, протягом визначеного у приписі строку.

Кваліфікований надавач зобов'язаний у визначений у приписі про усунення порушень строк письмово подати до КО інформацію про усунення порушень разом із 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 кваліфікованого надавача (найменування, ідентифікаційні дані та контактна інформація);
- сфера оцінки відповідності;
- перелік кваліфікованих електронних довірчих послуг, які має намір надавати КНЕДП ЗС України;
- 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 оцінки 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 кваліфікований надавач повинен повідомити КО шляхом надання копій документів про відповідність (за наявності) та аудиторських звітів не пізніше трьох робочих днів із дня їх отримання.

ООВ надає публічний доступ до актуальної інформації про результати оцінки відповідності у сфері електронних довірчих послуг.

8.6.4. Оформлення результатів оцінювання (аудиту) системи захисту інформації

За результатами проведених робіт оцінювач (експерт, аудитор) складає звіт з оцінювання реалізації заходів захисту.

За результатами позитивного оцінювання КНЕДП ЗС України отримує сертифікат відповідності стандарту інформаційної безпеки та/або надсилає авторизаційний лист до Адміністрації Державної служби спеціального зв'язку та захисту інформації України для включення до переліку авторизованих систем із безпеки.

8.7. Самоперевірки

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

9. ІНШІ КОМЕРЦІЙНІ ТА ЮРИДИЧНІ ПИТАННЯ

До об'єктів, процесів і заходів, зазначених у 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

Формування кваліфікованого сертифіката здійснюється для користувачів (працівників) установ, що відносяться до сфери управління Міністерства оборони України та/або підпорядковані (придані) військовому командуванню Збройних Сил України, для виконання своїх посадових обов'язків на безоплатній основі.

Зміна статусу кваліфікованого сертифіката здійснюється на безоплатній основі.

9.1.2. Плата за доступ до сертифіката

Плата за доступ до кваліфікованого сертифіката відсутня.

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

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

9.1.4. Плата за інші послуги

Для працівників установ, що відносяться до сфери управління Міністерства оборони України та/або підпорядковані (придані) військовому командуванню Збройних Сил України, послуги надаються на безоплатній основі.

9.1.5. Політика відшкодування

КНЕДП ЗС України не відшкодовує рахунки на послуги, що були надані на безоплатній основі.

9.2. Фінансова відповідальність

Діяльність КНЕДП ЗС України відповідає вимогам частини п'ятої статті 16 Закону щодо надання кваліфікованих електронних довірчих послуг, за умови внесення коштів на поточний рахунок зі спеціальним режимом використання в 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 зі спеціальним режимом використання в 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

У процесі надання послуг КНЕДП ЗС України обробляє конфіденційну інформацію, яка не оприлюднюється для загального ознайомлення. Захист конфіденційної інформації здійснюється згідно з чинним законодавством.

9.4. Інформація, що не належить до конфіденційної

Інформація та документація, яка є доступною для загального ознайомлення, публікується на вебсайті КНЕДП ЗС України та не належить до конфіденційної інформації.

9.4.1. Відповідальність за захист конфіденційної інформації

КНЕДП ЗС України здійснює захист конфіденційної інформації та несе відповідальність згідно з вимогами чинного законодавства.

9.5. Конфіденційність персональної даних

9.5.1. Концепція захисту персональних даних

КНЕДП ЗС України у процесі надання кваліфікованих електронних довірчих послуг здійснює:

- захист персональних даних користувачів відповідно до вимог Закону України “Про захист персональних даних” і відомчих керівних документів;
- інформування КО та, у 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 із моменту, коли йому стало відомо про таке порушення.

9.5.2. Визначення персональних даних

Поняття “персональні дані” розуміється у значенні, наведеному в статті 2 Закону України “Про захист персональних даних”.

9.5.3. Персональні дані, що не вважаються конфіденційними

Персональні дані можуть відноситись до відкритої інформації у випадках, визначених чинним законодавством.

9.5.4. Відповідальність за захист персональних даних

КНЕДП ЗС України гарантує дотримання вимог законодавства про захист персональних даних і несе відповідальність згідно з вимогами чинного законодавства.

Керівник КНЕДП ЗС України забезпечує створення умов для безперервної особистої освіти та постійне підвищення кваліфікації

персоналу КНЕДП ЗС України у сферах інформаційних технологій, захисту інформації та персональних даних.

9.5.5. Інформація та згода на використання персональних даних

Відповідно до Закону України "Про захист персональних даних" КНЕДП ЗС України надає кваліфіковані електронні довірчі послуги відповідно до отриманих у встановленому порядку карток з реєстраційними даними (заявок) від користувачів і здійснює обробку персональних даних на підставі наданої користувачами згоди на обробку персональних даних.

9.5.6. Розкриття персональних даних

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

Керівник КНЕДП ЗС України та персонал КНЕДП ЗС України дотримуються вимог законодавства України у сфері захисту персональних даних.

9.6. Права інтелектуальної власності

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

9.7. Зобов'язання та гарантії

9.7.1. Зобов'язання та гарантії кваліфікованого надавача

КНЕДП ЗС України надає кваліфіковані електронні довірчі послуги з дотриманням вимог законодавства у сфері електронних довірчих послуг, Регламенту роботи КНЕДП ЗС України, цієї Політики сертифіката та Положень сертифікаційних практик КНЕДП ЗС України.

9.7.2. Зобов'язання та гарантії відокремлених пунктів реєстрації

Відокремлені пункти реєстрації КНЕДП ЗС України здійснюють реєстрацію користувачів на підставі рішень військового керівництва ЗС України. ВПР виконують свої функції відповідно до Регламенту роботи КНЕДП ЗС України, цієї Політики сертифіката та Положень сертифікаційних практик КНЕДП ЗС України. З усіх питань надання кваліфікованих електронних довірчих послуг ВПР підпорядковуються КНЕДП ЗС України та мають виконувати вимоги та розпорядження його керівника.

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

9.7.3. Зобов'язання та гарантії користувачів

Користувачі зобов'язані:

- забезпечувати конфіденційність і неможливість доступу інших осіб до особистого ключа;
- невідкладно повідомляти КНЕДП ЗС України про підозру або факт компрометації особистого ключа;
- надавати достовірну інформацію, необхідну для отримання електронних довірчих послуг;
- своєчасно надавати КНЕДП ЗС України інформацію про зміну ідентифікаційних даних, які містить кваліфікований сертифікат;

- не використовувати особистий ключ у разі його компрометації, а також в 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 і пароль до нього (атрибути захисту від доступу сторонніх осіб до параметрів особистого ключа) не скомпрометовані та не використовуються іншими особами;
- уся інформація, зазначена в кваліфікованому сертифікаті, є коректною;
- кваліфікований сертифікат використовується за призначенням відповідно до положень цієї Політики сертифіката;

9.7.4. Зобов’язання та гарантії суб’єктів, які довіряють кваліфікованому надавачу

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

9.7.5. Зобов’язання та гарантії інших учасників

ЦЗО, перш ніж прийняти рішення про внесення КНЕДП ЗС України до Довірчого списку та надання йому кваліфікованого статусу, повинен пересвідчитися в наявності у КНЕДП ЗС України:

- документа, що підтверджує відповідність системи захисту інформації КНЕДП ЗС України вимогам положень статті 8 Закону України “Про захист інформації в інформаційно-комунікаційних системах”;
- документів, які підтверджують право власності та право користування КНЕДП ЗС України нежилими приміщеннями, які використовуються для розміщення всіх складових програмно-технічного комплексу, що забезпечують надання кваліфікованих електронних довірчих послуг;
- належного персоналу КНЕДП ЗС України;
- документів, які підтверджують освітньо-кваліфікаційний рівень і трирічний стаж роботи за фахом персоналу КНЕДП ЗС України;
- документів, які підтверджують право власності або право користування ЗКЕП, які використовуються КНЕДП ЗС України для надання кваліфікованих електронних довірчих послуг;
- документів, що підтверджують внесення коштів на поточний рахунок КНЕДП ЗС України зі спеціальним режимом використання в банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) із необхідним обсягом коштів або чинного договору страхування цивільно-правової відповідальності з необхідним розміром страхової суми, що встановлені Законом, для забезпечення відшкодування збитків, які можуть бути заподіяні користувачам унаслідок неналежного виконання КНЕДП ЗС України своїх обов’язків;

- наявності Регламенту роботи КНЕДП ЗС України, цієї Політики сертифіката та Положень сертифікаційних практик КНЕДП ЗС України.

9.8. Відмова від відповідальності

КНЕДП ЗС України, користувачі, суб'єкти, які довіряють КНЕДП ЗС України, та інші сторони не можуть відмовитися від гарантій, передбачених пунктом 9.7 цієї Політики сертифіката.

9.9. Обмеження відповідальності

У разі якщо КНЕДП ЗС України 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 із порушенням зазначених обмежень.

9.10. Відшкодування збитків

Відшкодування збитків, які можуть бути завдані користувачам електронних довірчих послуг чи третім особам унаслідок неналежного виконання КНЕДП ЗС України своїх зобов'язань здійснюється відповідно до вимог чинного законодавства України.

9.11. 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 ЗС України.

9.12. Індивідуальні повідомлення та комунікації з учасниками інфраструктури відкритих ключів

КНЕДП ЗС України здійснює комунікацію з учасниками інфраструктури відкритих ключів шляхом:

- розміщення повідомлень та оголошень на вебсайті КНЕДП ЗС України;
- інформування ЦЗО, КО та органу з питань захисту персональних даних шляхом надсилання повідомлень у паперовій та електронній формах;
- доведення повідомлень та оголошень, що містять інформацію з обмеженим доступом, до учасників інфраструктури відкритих ключів в установленому законодавством порядку.

9.13. Зміни

Внесення змін до цієї Політики сертифіката здійснюється в разі:

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

Нові версії цієї Політики сертифіката публікуються на вебсайті КНЕДП ЗС України.

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

9.14. Положення щодо вирішення спорів

У випадку виникнення спорів або розбіжностей КНЕДП ЗС України

вирішує їх шляхом переговорів і консультацій з учасниками інфраструктури відкритих ключів.

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

9.15. Застосовне право

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

9.16. Дотримання чинного законодавства

Під час надання електронних довірчих послуг КНЕДП ЗС України 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 27.01.2010 № 55 “Про впорядкування транслітерації українського алфавіту латиницею”;
- постанови 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”;
- постанови Кабінету Міністрів України від 10.12.2024 № 1408 “Деякі питання зберігання документованої інформації та її передавання до центрального засвідчувального органу в разі припинення діяльності кваліфікованого надавача електронних довірчих послуг”;
- постанови Кабінету Міністрів України від 28.06.2024 № 764 “Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг”;
- постанови Кабінету Міністрів України від 12.12.2023 № 1298 “Про затвердження вимог до форматів удосконалених електронних підписів та печаток, які використовуються для надання електронних публічних послуг, та вимог до створення та перевірки удосконалених електронних підписів та печаток, що базуються на кваліфікованих сертифікатах відкритих ключів”;
- постанови Кабінету Міністрів України від 13.09.2024 № 1062 “Про затвердження Порядку проведення процедури оцінки відповідності у сферах електронної ідентифікації та електронних довірчих послуг”;
- наказу Міністерства юстиції України, Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 01.02.2019 № 316/5/57 “Про позначку кваліфікованого сертифіката відкритого ключа”, зареєстрованого в Міністерстві юстиції України 05.02.2019 за № 123/33094;
- наказу Міністерства цифрової трансформації України від 17.11.2023 № 149 “Про затвердження Порядку ведення реєстру чинних, блокованих і скасованих сертифікатів відкритих ключів, які сформовані центральним засвідчувальним органом”, зареєстрованого в Міністерстві юстиції України

05 грудня 2023 року за № 2110/41166;

- наказ Міністерства цифрової трансформації України від 25.10.2025 № 173 “Вимоги 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 06.11.2025 за № 1625/45031;
- наказу Міністерства цифрової трансформації України від 06.04.2024 № 54 “Про затвердження форми плану припинення діяльності з надання кваліфікованих електронних довірчих послуг”, зареєстрованого в Міністерстві юстиції України 23.04.2024 за № 588/41933;
- наказу Міністерства цифрової трансформації України від 28.02.2024 № 33 “Про затвердження Регламенту роботи центрального засвідчувального органу”, зареєстрованого в Міністерстві юстиції України 15.03.2024 за № 393/41738;
- наказу Міністерства цифрової трансформації України від 28 грудня 2023 року № Н191 “Деякі питання реалізації вимог стандартів, у тому числі щодо забезпечення сумісності”.

Командир військової частини А0136
полковник Віталій КІНЧЕВСЬКИЙ

Додаток 2
до Регламенту роботи кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України"

ПОЛОЖЕННЯ СЕРТИФІКАЦІЙНИХ ПРАКТИК КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ "ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ ЗБРОЙНИХ СИЛ УКРАЇНИ"

щодо кваліфікованих сертифікатів електронного підпису та печатки

Київ 2026

ЗМІСТ

1. ВСТУП

1.1. Огляд

Ці Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України" щодо кваліфікованих сертифікатів електронного підпису та печатки (далі – Положення) визначають перелік практичних дій і процедур щодо кваліфікованих сертифікатів відкритих ключів (далі – кваліфіковані сертифікати) підписувачів і створювачів електронних печаток, що застосовуються кваліфікованим надавачем електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України" (далі – КНЕДП ЗС України) для реалізації Політики сертифіката кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України" (додаток 1 до Регламенту роботи КНЕДП ЗС України) (далі – Політика сертифіката КНЕДП ЗС України).

Дотримання практичних дій і процедур, визначених у цих Положеннях, є обов'язковим для керівника КНЕДП ЗС України, посадових осіб КНЕДП ЗС України та його відокремлених пунктів реєстрації (далі – ВПР), обов'язки яких безпосередньо пов'язані з реєстрацією користувачів, формуванням та обслуговуванням кваліфікованих сертифікатів.

Дотримання користувачами вимог, визначених у цих Положеннях, є обов'язковою умовою для надання електронних довірчих послуг.

Перелік усіх правил, що застосовуються КНЕДП ЗС України у процесі реєстрації користувачів, формування й обслуговування кваліфікованих сертифікатів КНЕДП ЗС України та користувачів, у тому числі управління їх статусом (блокування, поновлення та скасування), визначається Політикою сертифіката КНЕДП ЗС України.

Ці Положення 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

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: Положення сертифікаційних практик кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України" щодо кваліфікованих сертифікатів електронного підпису та печатки.

Скорочена назва документа: Положення сертифікаційних практик КНЕДП ЗС України".

Версія: 1.0.

Кваліфіковані сертифікати, сформовані КНЕДП ЗС України, містять визначений об’єктний ідентифікатор (OID), який використовується суб’єктами, які довіряють і здійснюють перевірку та підтвердження кваліфікованого електронного підпису чи печатки за допомогою кваліфікованого сертифіката, для визначення його придатності та надійності під час автентифікації користувачів.

1.3. Учасники інфраструктури відкритих ключів

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

1.3.1. Кваліфікований надавач

Відомості про КНЕДП ЗС України внесено до Довірчого списку відповідно до частини першої статті 30 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”.

КНЕДП ЗС України надає кваліфіковані електронні довірчі послуги з дотриманням вимог чинного законодавства, зокрема здійснює реєстрацію користувачів, формування та обслуговування їхніх кваліфікованих сертифікатів, а також управління їхнім статусом (блокування, поновлення та скасування).

КНЕДП ЗС України здійснює реєстрацію користувачів самостійно та/або через ВПР КНЕДП ЗС України.

1.3.2. Органи реєстрації

ВПР КНЕДП ЗС України є органами, що здійснюють реєстрацію користувачів. Вони представлені окремими підрозділами КНЕДП ЗС України та здійснюють реєстрацію користувачів із дотриманням вимог чинного законодавства та Регламенту роботи КНЕДП ЗС України.

Безпосередню реєстрацію користувачів у ВПР КНЕДП ЗС України здійснюють працівники, на яких покладено обов’язки з реєстрації користувачів (далі – віддалений адміністратор реєстрації).

До посадових осіб ВПР КНЕДП ЗС України, на яких покладено обов’язки з реєстрації користувачів, застосовуються такі ж вимоги, як і до адміністраторів реєстрації, визначених у пункті 5.3.1.2 Політики сертифіката КНЕДП ЗС України.

1.3.3. Користувачі

Користувачами кваліфікованих електронних довірчих послуг КНЕДП ЗС України та його ВПР у відповідності до вимог Закону України “Про електронну ідентифікацію та електронні довірчі послуги” та інших нормативних-правових актів у сферах електронної ідентифікації, електронних довірчих послуг та захисту інформації є: підписувачі, створювачі електронних печаток та особи, відповідальні за криптографічні ключі.

1.3.4. Суб’єкти, які довіряють

Фізичні та юридичні особи, а також їхні інформаційно-комунікаційні системи є суб’єктами, які довіряють КНЕДП ЗС України та використовують кваліфіковані сертифікати користувачів із метою їх автентифікації, зокрема шляхом перевірки та підтвердження електронного підпису чи печатки.

1.3.5. Інші учасники

Іншими учасниками у сфері електронних довірчих послуг є ЦЗО, КО,

ООВ, а також юридичні особи, які забезпечують на договірних засадах супроводження та технічну підтримку програмно-технічного комплексу ІКС КНЕДП ЗС України.

До інших учасників також можуть належати фізичні та юридичні особи, які прямо чи опосередковано пов’язані з формуванням та/або обслуговуванням кваліфікованих сертифікатів КНЕДП ЗС України та користувачів.

Пункт 1.3.5 Політики сертифіката КНЕДП ЗС України 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 ЗС України дозволено використовувати для:

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

Для визначення сфери використання кваліфікованого сертифіката КНЕДП ЗС України під час його формування встановлює розширення – призначення відкритого ключа “keyUsage”:

- digitalSignature + nonRepudiation або keyAgreement (цифровий підпис + неспростовність або узгодження ключа) – автентифікація;
- digitalSignature + nonRepudiation (цифровий підпис + неспростовність) – створення, перевірка та підтвердження кваліфікованого електронного підпису;
- digitalSignature + nonRepudiation (цифровий підпис + неспростовність) – створення, перевірка та підтвердження кваліфікованої електронної печатки;
- keyAgreement (узгодження ключа) – узгодження ключа шифрування.

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

Для перевірки кваліфікованої електронної печатки під час формування кваліфікованого сертифіката КНЕДП ЗС України встановлює додаткове розширення – уточнене призначення відкритого ключа “extendedKeyUsage” із об’єктним ідентифікатором (OID): 1.2.804.2.1.1.1.3.9.

На користувачів покладається відповідальність за використання ними ПЗ, яке правильно інтерпретує, відображає та використовує інформацію та обмеження, закодовані в кваліфікованих сертифікатах.

1.4.1.1. Види сертифікатів

Відповідно до цих Положень формує кваліфіковані сертифікати таких типів:

- кваліфікований сертифікат електронного підпису, що пов’язує відкритий ключ кваліфікованого електронного підпису з фізичною особою або

технічним засобом (складовою ІКС, засобом КЗІ тощо) та підтверджує їхні ідентифікаційні дані під час створення, перевірки та підтвердження кваліфікованого електронного підпису, а також автентифікації;

- кваліфікований сертифікат електронної печатки, що пов'язує відкритий ключ кваліфікованої електронної печатки з установою та підтверджує її ідентифікаційні дані під час створення, перевірки та підтвердження кваліфікованої електронної печатки, а також автентифікації;
- кваліфікований сертифікат шифрування, що пов'язує відкритий ключ кваліфікованого електронного підпису чи печатки з фізичною особою або технічним засобом (складовою ІКС, засобом КЗІ тощо) в установі та забезпечує направлене шифрування під час обміну інформацією;
- кваліфікований сертифікат автентифікації вебсайту, що пов'язує відкритий ключ кваліфікованого електронного підпису з установою, що є володільцем або розпорядником мережевого ресурсу (вебсайту або доменного імені) та забезпечує автентифікацію установи власника (розпорядника) вебсайту та шифрування інформації між учасником онлайн-операції та вебсайтом.

Формування кваліфікованих сертифікатів КНЕДП ЗС України для технічних засобів інформаційно-комунікаційних систем здійснюється виключно програмно-технічними засобами криптографічного захисту інформації на ЗКЕП, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації, отриманий на ці засоби від Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

1.4.1.2. Строк дії сертифікатів

Кваліфіковані сертифікати КНЕДП ЗС України формуються ЦЗО зі строком дії не більше 5 років.

Кваліфіковані сертифікати користувачів формуються КНЕДП ЗС України зі строком дії до 2 років.

Пункт 1.4.1.2 Політики сертифіката КНЕДП ЗС України містить додаткову інформацію.

1.4.2. Заборонене використання сертифіката

Не допускається використання кваліфікованого сертифіката, сформованого КНЕДП ЗС України, у сферах, які не відповідають зазначеному у кваліфікованому сертифікаті призначенню відкритого ключа "keyUsage".

1.5. Управління Положеннями

1.5.1. Відповідальність за Положення

Реквізити Кваліфікованого надавача електронних довірчих послуг "Центр сертифікації ключів Збройних Сил України":

Код ЄДРПОУ: 22991050

Місцезнаходження: 03168, м. Київ, просп. Повітряних Сил, 6.

Контактний телефон: +38 (044) 454 41 06, (62) 232 06, (62) 234 78

Адреса електронної пошти: manager@ca.mil.gov.ua

Адреса вебсайту: https://ca.mil.gov.ua

Ці Положення підтримуються КНЕДП ЗС України, містять усю необхідну

інформацію та структуровані відповідно до RFC 3647 “Інфраструктура відкритих ключів Інтернету X.509 Політика сертифікатів і практика сертифікації”.

Ці Положення, а також зміни до них затверджуються начальником Генерального штабу Збройних Сил України.

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

1.5.2. Внесення змін до Положень

Зміни вносяться відповідно до пункту 9.12 цих Положень.

1.6. Визначення термінів і перелік скорочень

1.6.1. Визначення термінів

У цих Положеннях терміни застосовуються у наступних значеннях:

відповідальна особа – посадова особа (посадові особи) або структурний підрозділ, визначені наказом керівника установи, які виконують функції з організації використання кваліфікованих електронних довірчих послуг та мають повноваження щодо подання документів, необхідних для їх отримання у КНЕДП ЗС України;

доменне ім’я – символьне позначення для адресації вузлів мережі та мережевих ресурсів (вебсайтів, серверів електронної пошти, мережевих серверів тощо) в зручній для людини формі;

заявник – користувач, фізична або посадова особа, яка звернулась у встановленому порядку до КНЕДП ЗС України чи його ВПР з метою отримання кваліфікованих електронних довірчих послуг;

ідентифікація особи – процес використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, у результаті якого забезпечується однозначне встановлення фізичної, юридичної особи або відповідальної особи (уповноваженого представника установи);

кваліфікований сертифікат відкритого ключа – сертифікат відкритого ключа, який засвідчує чинність і належність відкритого ключа підписувачу та видається кваліфікованим надавачем електронних довірчих послуг. Сертифікати ключів розповсюджуються в електронній формі або у формі документа на папері;

особи, відповідальні за криптографічні ключі – представники підрозділу з кіберзахисту (служби захисту інформації), криптографічного захисту інформації або призначені особи в установі, відповідальні за генерацію, застосування та збереження криптографічних ключів для програмних, апаратних засобів, персоналу, мережевих ресурсів (вебсайту або доменного імені) інформаційних, комунікаційних, інформаційно-комунікаційних систем та/або засобів (систем) криптографічного захисту інформації;

особистий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки та доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених

стандартами для кваліфікованих сертифікатів;

підписувачі – фізичні особи, представники установи (військовослужбовці, державні службовці та працівники), які створюють та застосовують кваліфікований електронний підпис для виконання функцій у межах своїх посадових обов'язків;

позаштатний адміністратор реєстрації – посадова особа (посадові особи) установи (керівник, або визначений представник кадрового органу), що здійснює в установі функцію ідентифікації особи користувача, підтвердження володіння ним особистим ключем і перевірку його повноважень;

посадові особи – це військовослужбовці, державні службовці та працівники установ, які виконують організаційно-розпорядчі або адміністративно-господарські функції в межах своїх службових (посадових) обов'язків;

реєстрація – внесення відомостей про заявника, підписувача, створювача електронної печатки чи технічного засобу до бази КНЕДП ЗС України;

розпорядник вебсайту (доменного імені, інформаційного ресурсу) – установа, якій надано право управляти (розпоряджатися) вебсайтом (доменним іменем, інформаційним ресурсом);

створювачі електронних печаток – установи (юридичні особи), які створюють електронну печатку;

установа – орган військового управління, військова частина, установа або організація, військовий навчальний заклад, територіальний центр комплектування та соціальної підтримки та всі інші юридичні особи, що відносяться до сфери управління Міністерства оборони України та/або підпорядковані (придані) військовому командуванню Збройних Сил України;

фізичні особи – військовослужбовці, державні службовці та працівники установ, що діють в інтересах обороноздатності держави.

Інші 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 № 764 "Деякі питання дотримання вимог у сферах електронної ідентифікації та електронних довірчих послуг", інших нормативно-правових актах у сферах електронних довірчих послуг, криптографічного та технічного захисту інформації, електронних комунікацій.

1.6.2. Перелік скорочень

ВПР	Відокремлений пункт реєстрації
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань
ЄДДР	Єдиний державний демографічний реєстр

ЄДРПОУ	Єдиний державний реєстр підприємств та організацій України
ЗКЕП	Засіб кваліфікованого електронного підпису чи печатки
ІКС	Інформаційно-комунікаційна система
КЕП	Кваліфікований електронний підпис
КЗІ	Криптографічний захист інформації
КНЕДП ЗС України	Кваліфікований надавач електронних довірчих послуг “Центр сертифікації ключів Збройних Сил України”
КО	Контролюючий орган
НБУ	Національний банк України
ООВ	Орган з оцінки відповідності
ПДФО	Податок на доходи фізичних осіб
ПЗ	Програмне забезпечення
РНОКПП	Реєстраційний номер облікової картки платника податків
СПФМ	Суб’єкт первинного фінансового моніторингу
УНЗР	Унікальний номер запису в ЄДДР
ЦЗО	Центральний засвідчувальний орган
DNS	Domain Name System
OCSP	Online Certificate Status Protocol
OID	Object identifier
TSP	Time Stamp Protocol
CRL	Certificate Revocation List
CMP	Certificate Management Protocol
UPN	User Principal Name

2. ОБОВ’ЯЗКИ ЩОДО ПУБЛІКАЦІЇ ТА ЗБЕРІГАННЯ

До об’єктів, процесів і заходів, зазначених у 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 ЗС України через свій вебсайт (https://ca.mil.gov.ua) забезпечує вільний доступ до:

- відомостей про КНЕДП ЗС України;
- даних про внесення відомостей про КНЕДП ЗС України до Довірчого списку;
- положень Регламенту КНЕДП ЗС України, Політики сертифіката КНЕДП ЗС України та цих Положень;
- актів законодавства у сфері електронних довірчих послуг;
- кваліфікованих сертифікатів КНЕДП ЗС України;
- переліку кваліфікованих електронних довірчих послуг, які надає КНЕДП ЗС України;
- даних про ЗКЕП, що використовуються під час надання кваліфікованих електронних довірчих послуг КНЕДП ЗС України;
- порядку надання кваліфікованих електронних довірчих послуг;
- переліку та форм документів, на підставі яких надаються кваліфіковані електронні довірчі послуги;

- переліку та відомостей про ВПР КНЕДП ЗС України;
- реєстру чинних, блокованих і скасованих кваліфікованих сертифікатів;
- відомостей про обмеження під час використання кваліфікованих сертифікатів користувачами;
- даних про порядок перевірки чинності кваліфікованого сертифіката, у тому числі умови перевірки статусу сертифіката.

Ці Положення доступні цілодобово у форматі лише для читання на вебсайті КНЕДП ЗС України (https://ca.mil.gov.ua).

2.2. Публікація інформації

2.2.1. Публікація сертифікатів користувачів

КНЕДП ЗС України забезпечує вільний доступ до реєстру чинних, блокованих і скасованих кваліфікованих сертифікатів через власний вебсайт (https://ca.mil.gov.ua).

Адміністратор сертифікації КНЕДП ЗС України забезпечує публікацію кваліфікованих сертифікатів користувачів, згода на публікацію яких надана такими користувачами, та списків відкликаних сертифікатів (CRL) на вебсайті кваліфікованого надавача.

Згода на публікацію кваліфікованого сертифіката надається користувачем під час подання картки з реєстраційними даними (заявки) на формування кваліфікованого сертифіката.

Кваліфікований надавач може визначати та встановлювати обмеження щодо публікації кваліфікованих сертифікатів користувачів на вебсайті КНЕДП ЗС України.

2.2.2. Публікація сертифікатів кваліфікованого надавача

КНЕДП ЗС України забезпечує вільний доступ до інформації про кваліфіковані сертифікати КНЕДП ЗС України через власний вебсайт (https://ca.mil.gov.ua).

Відомості про кваліфіковані сертифікати КНЕДП ЗС України, сформовані з використанням самопідписаного сертифіката електронної печатки ЦЗО, статус та обмеження у використанні таких сертифікатів, а також списки відкликаних сертифікатів (CRL) містяться в реєстрі чинних, блокованих і скасованих кваліфікованих сертифікатів, що ведеться центральним засвідчувальним органом (https://czo.gov.ua).

2.2.3. Доступ до сертифікатів користувачів

КНЕДП ЗС України 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 їхніх кваліфікованих сертифікатів.

Кваліфікований надавач може визначати та встановлювати обмеження щодо публікації кваліфікованих сертифікатів користувачів на вебсайті КНЕДП ЗС України.

2.2.4. Строк закінчення дії сертифіката

Дата та час початку та закінчення строку дії кваліфікованого сертифіката зазначається в 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 і періодичність публікації

КНЕДП ЗС України забезпечує актуальність та своєчасну публікацію інформації на своєму вебсайті, зокрема:

- про КНЕДП ЗС України та його ВПР;
- положень Регламенту КНЕДП ЗС України, Політики сертифіката КНЕДП ЗС України та цих Положень;
- нормативно-правових актів у сфері електронних довірчих послуг;
- кваліфікованих сертифікатів КНЕДП ЗС України та користувачів;
- списків відкликаних сертифікатів.

КНЕДП ЗС України 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 ЗС України.

Публікація списків відкликаних сертифікатів відбувається в автоматичному режимі.

Час зміни статусу кваліфікованих сертифікатів синхронізований зі 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 і містить інформацію про всі відкликані кваліфіковані сертифікати, які були сформовані КНЕДП ЗС України.

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 і часом формування поточного часткового списку відкликаних сертифікатів.

2.4. Контроль доступу до репозиторію / вебсайту

КНЕДП ЗС України забезпечує цілодобове функціонування власного вебсайту, актуальність і доступність інформації на ньому.

Доступ лише для читання необмежений.

Користувач може знайти інформацію про свій кваліфікований сертифікат шляхом здійснення його пошуку на вебсайті КНЕДП ЗС України в розділі “Пошук”, зазначивши у відповідних вкладках інформацію про код ЄДРПОУ установи та реквізити власника, а саме РНОКПП (у разі відсутності серія (за наявності) та номер паспорта).

Пункт 2.4. Політики сертифіката КНЕДП ЗС України містить додаткову інформацію.

3. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

До об’єктів, процесів і заходів, зазначених у 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 ЗС України 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 ЗС України, 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) користувача;
   - 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);
   - найменування створювача електронної печатки та код згідно з ЄДРПОУ;
5. значення відкритого ключа, який відповідає особистому ключу;
6. відомості про початок і закінчення строку дії кваліфікованого сертифіката;
7. серійний номер кваліфікованого сертифіката, унікальний для КНЕДП ЗС України;
8. кваліфікований електронний підпис або кваліфіковану електронну печатку, створені КНЕДП ЗС України;
9. відомості про місце розміщення кваліфікованого сертифіката, за допомогою якого перевіряється кваліфікований електронний підпис або кваліфікована електронна печатка, зазначені в пункті 8;
10. відомості про місце надання послуги перевірки статусу відповідного кваліфікованого сертифіката;
11. зазначення про те, що особистий ключ, пов’язаний із відкритим ключем, зберігається в ЗКЕП 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 у кваліфікованих сертифікатах, відповідають

позначення (реквізити, атрибути), визначені у стандартах щодо профілів сертифікатів відповідно до пункту 7.1 Політики сертифіката КНЕДП ЗС України.

Пункт 3.1 Політики сертифіката КНЕДП ЗС України містить 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 Політики сертифіката КНЕДП ЗС України.

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 ЗС України.

3.1.3. Анонімність або використання псевдонімів

Використання псевдонімів здійснюється відповідно до пункту 3.1.3 Політики сертифіката КНЕДП ЗС України.

3.1.4. Правила інтерпретації різних форм позначень сертифіката

Міжнародні літери повинні кодуватися згідно з UTF-8.

3.1.5. Унікальність позначень сертифіката

КНЕДП ЗС України 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

Підтвердження володіння підписувачем особистим ключем, відповідний якому відкритий ключ надається на сертифікацію, здійснюється під час надання допомоги підписувачу у процесі генерації ключової пари без розкриття особистого ключа заявника:

- у кваліфікованого надавача або його ВПР – адміністратором реєстрації (віддаленим адміністратором реєстрації);
- в установі – позаштатним адміністратором реєстрації або відповідальною особою.

Пункт 3.2.1 Політики сертифіката КНЕДП ЗС України містить додаткову інформацію щодо методів підтвердження володіння користувачем особистим ключем.

3.2.2. Ідентифікація особи

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

У випадках, коли заявники та підписувачі не мають змоги прибути до кваліфікованого надавача чи його ВПР, ідентифікація проводиться в установі позаштатним адміністратором реєстрації. Для підтвердження повноважень

позаштатного адміністратора реєстрації кваліфікованому надавачу та його ВПР надсилається витяг із наказу керівника установи, що підтверджує такі повноваження, або копія відповідного наказу, завірена в установленому порядку керівником або визначеними ним представниками.

Особи, які звернулися у встановленому порядку до КНЕДП ЗС України для отримання послуги з формування та видачі кваліфікованого сертифіката, надають ідентифікаційні дані, які вносяться до кваліфікованого сертифіката.

Ідентифікаційні дані, які однозначно визначають особу, заповнюються в картці з реєстраційними даними (заявці) на отримання кваліфікованих сертифікатів і вносяться до кваліфікованого сертифіката. Механізми їх підтвердження викладено в Таблицях 3 та 4.

Таблиця 3. Обов'язкові ідентифікаційні дані та механізми їх підтвердження під час ідентифікації користувачів, які вперше звернулися за отриманням послуги формування кваліфікованого сертифіката

Ідентифікаційні дані	**Обов'язковість надання даних**	**Механізми підтвердження ідентифікаційних даних**
Прізвище, ім'я, по батькові (за наявності)	Обов'язково	Документальне (паспорт)
РНОКПП (за наявності)	Обов'язково	Документальне (облікова картка платника податків, паспорт)
Серія (за наявності), номер паспорта	Обов'язково для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття РНОКПП[1]	Документальне (паспорт)
Відомості щодо належності користувача до установи та/або його повноваження щодо виконання функцій в інтересах установи	Обов'язково	Документальне (оформлені встановленим порядком: список посадових осіб установи; довідка, яка підтверджує факт перебування на військовій службі (роботі) (форма 5 або форма 6); витяг із наказу.

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

Ідентифікаційні дані	**Обов'язковість надання даних**	**Механізми підтвердження ідентифікаційних даних**
Найменування юридичної особи	Обов'язково	Документальне (відповідно до зазначеного в довідці з ЄДРПОУ)

[1] 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

Ідентифікаційні дані	Обов'язковість надання даних	Механізми підтвердження ідентифікаційних даних
Код згідно з ЄДРПОУ	Обов'язково	Документальне (відповідно до зазначеного в довідці з ЄДРПОУ)
Місцезнаходження	Обов'язково	Документальне (відповідно до зазначеного в довідці з ЄДРПОУ)

Переліки, форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги, та роз'яснення щодо їх оформлення публікуються на вебсайті кваліфікованого надавача за посиланням https://ca.mil.gov.ua/registration-documents.

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

- без залучення додаткових пристроїв шляхом візуального зіставлення однакової інформації (значення "документ №", "дата народження", "строк дії"), яка надрукована в зоні візуальної перевірки та машинозчитувальній зоні;
- шляхом автоматизованого зчитування інформації з використанням апаратних і програмних засобів (зчитувачів), оснащених інтерфейсами взаємодії, визначеними державним підприємством "Поліграфічний комбінат "Україна" (перелік і вимоги до яких опубліковані на офіційному вебсайті).

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

Для підтвердження належного проведення процедури ідентифікації користувача КНЕДП ЗС України забезпечує зберігання реєстраційних карток (заявок) на формування або зміну статусу кваліфікованих сертифікатів і копій документів, які надавались користувачами під час їх ідентифікації. Копії таких документів зберігаються в паперовому вигляді в приміщеннях кваліфікованого надавача або його ВПР або в електронній формі з використанням захищеної системи електронного документообігу Міністерства оборони України.

Дані, які використовувались у процедурі ідентифікації заявника, засвідчуються за правилами, наведеними в Таблиці 5.

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

Форма документа	Засвідчення з боку заявника		Засвідчення з боку кваліфікованого надавача	
	Тип підпису	Черга засвідчення	Тип підпису	Черга засвідчення
Паперова	Власноручний	Перша	Штамп адміністратора реєстрації та власноручний	Друга

Форма документа	Засвідчення з боку заявника		Засвідчення з боку кваліфікованого надавача	
	Тип підпису	Черга засвідчення	Тип підпису	Черга засвідчення
	підпис		підпис із зазначенням прізвища та ініціалів	
Електронна	Кваліфікований електронний підпис із використанням чинного КЕП	Перша	Кваліфікований електронний підпис адміністратора реєстрації	Друга

Формування та видача кваліфікованого сертифіката без ідентифікації користувача та/або представника установи, дані яких міститимуться у кваліфікованому сертифікаті, не допускається.

Засвідчення КНЕДП ЗС України карток із реєстраційними даними (заявок) без завершення встановлення особи заявника та без належного засвідчення ним документів не допускається.

3.2.3. Неперевірена інформація про користувача

Не допускається використання неверифікованої інформації про особу.

Відповідальний працівник КНЕДП ЗС України, на якого покладено виконання обов'язків адміністратора реєстрації (віддаленого адміністратора реєстрації), встановлює належність ідентифікаційних даних особі:

- за паспортом громадянина України або іншими документами, виданими відповідно до законодавства про ЄДДР;
- за допомогою інформації, що міститься в ЄДР, інформаційних системах (ресурсах) Міністерства внутрішніх справ України (сервіси "Пошук паспорта громадянина України серед викрадених та втрачених", "Перевірка недійсних документів").

3.2.4. Підтвердження повноважень

Під час ідентифікації заявника, відповідальної особи або особи, відповідальної за криптографічні ключі, посадова особа КНЕДП ЗС України, на яку покладено виконання обов'язків адміністратора реєстрації (віддаленого адміністратора реєстрації), здійснює ідентифікацію особи відповідно до пункту 3.2.2 Політики сертифіката КНЕДП ЗС України та проводить перевірку документів, що визначають її повноваження (наказ про призначення, розпорядження). При цьому, підтвердження повноважень посадових осіб кваліфікованого надавача здійснюється відповідно до розпорядчого документа (наказу) керівника КНЕДП ЗС України.

3.3. Ідентифікація та автентифікація за заявою на повторний ключ

3.3.1. Ідентифікація та автентифікація користувача за заявою про повторне формування кваліфікованого сертифіката відкритого ключа, за умови чинності попереднього кваліфікованого сертифіката, сформованого КНЕДП ЗС України

Під час повторного формування кваліфікованого сертифіката користувачу посадова особа КНЕДП ЗС України, на яку покладено виконання обов'язків адміністратора реєстрації (віддаленого адміністратора реєстрації), повинна

перевірити актуальність інформації, що надавалася користувачем під час попереднього формування кваліфікованого сертифіката.

У разі зміни ідентифікаційних даних, що містяться у кваліфікованому сертифікаті, користувач у триденний строк із дня настання таких змін надає до КНЕДП ЗС України або його ВПР документи, що підтверджують відповідні зміни, а також заявку про зміну статусу кваліфікованого сертифіката для скасування такого сертифіката та картку з реєстраційними даними (заявку) для формування кваліфікованого сертифіката з новими ідентифікаційними даними.

Під час дистанційного формування кваліфікованого сертифіката користувач, накладаючи кваліфікований електронний підпис чи печатку на картку з реєстраційними даними (заявку) та на відповідний електронний запит на формування сертифіката (далі – запит на сертифікат), тим самим підтверджує, що його ідентифікаційні дані залишаються незмінними.

Перевірка ідентифікаційних даних користувача та законності звернення щодо дистанційного формування кваліфікованого сертифіката здійснюється в ході ідентифікації й автентифікації користувача за раніше сформованим чинним на момент такого звернення кваліфікованим сертифікатом і підтвердженням його повноважень шляхом перевірки документів, що засвідчують його повноваження, або шляхом перевірки інформації у відповідних ІКС.

Повторне формування кваліфікованого сертифіката користувача не продовжує строк його дії.

3.3.2. Ідентифікація та автентифікація користувача у випадку звернення щодо формування нового кваліфікованого сертифіката відкритого ключа, у разі якщо попередній кваліфікований сертифікат, сформований КНЕДП ЗС України, скасовано або строк його дії закінчився

У разі якщо кваліфікований сертифікат користувача скасовано або строк дії такого сертифіката закінчився, для формування нового кваліфікованого сертифіката користувач подає документи відповідно до первинної процедури звернення (пункт 4.1 цих Положень).

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

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

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

Тип операції (причина подання заявки)	**Форма подання заявки**	**Механізми підтвердження ідентифікаційних даних**
Блокування кваліфікованого сертифіката	Усна	За ключовою фразою голосової автентифікації, первинний обмін якою між користувачем і кваліфікованим надавачем здійснюється під час подання картки з реєстраційними даними (заявки) на формування кваліфікованого сертифіката

Тип операції (причина подання заявки)	Форма подання заявки	Механізми підтвердження ідентифікаційних даних
	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 кваліфікованим надавачем
Скасування кваліфікованого сертифіката	Письмова паперова	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які вперше звернулися за отриманням послуги
	Письмова електронна	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які мають чинний кваліфікований сертифікат, сформований кваліфікованим надавачем
Поновлення кваліфікованого сертифіката	Письмова паперова	Механізми аналогічні підтвердженню ідентифікаційних даних користувачів, які вперше звернулися за отриманням послуги

3.5. Автентифікація в разі втрати засобу автентифікації

КНЕДП ЗС України не використовує номер телефону та/або адресу електронної пошти користувача як засоби автентифікації користувача для подання заявок про блокування або скасування кваліфікованого сертифіката.

Автентифікація користувача здійснюється за участі адміністратора реєстрації КНЕДП ЗС України або його ВПР за ключовою фразою голосової автентифікації.

4. ВИМОГИ ДО ЖИТТЄВОГО ЦИКЛУ СЕРТИФІКАТА

До об’єктів, процесів і заходів, зазначених у 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

Установи отримують від КНЕДП ЗС України або його ВПР електронні довірчі послуги за належним чином оформленими заявками від керівників установ, які надсилаються разом із додатками на адресу військової частини А0136.

Додатки до заявки:

- копія довідки про внесення установи (юридичної особи) до ЄДРПОУ, засвідчена в установленому порядку;
- витяг із наказу або завірена в установленому порядку копія наказу керівника установи про призначення особи, відповідальної за організацію використання кваліфікованих електронних довірчих послуг в установі.

Заявки від установ, які будуть отримувати електронні довірчі послуги у ВПР кваліфікованого надавача, розглядаються керівником КНЕДП ЗС України, відтак копії з резолюцією надсилаються до ВПР для їх подальшого відпрацювання.

У разі неналежного оформлення документів вони повертаються на доопрацювання в установленому порядку.

Заявка з додатками надсилається на адресу військової частини А0136 під час розгортання кваліфікованих електронних довірчих послуг в установі. З метою актуалізації даних та оновлення раніше поданої інформації така заявка від установи повторно надсилається кожні 3 роки з дати формування першої заявки.

У разі зміни відповідальних осіб вносяться зміни до чинного наказу або видається новий наказ із зазначенням у ньому про втрату чинності попереднього. Витяг із наказу або завірена в установленому порядку копія наказу надсилається до службового діловодства військової частини А0136 та до ВПР, у якому обслуговується установа, разом із супровідним листом.

У разі зміни ідентифікаційних даних установи, які вказані в довідці з ЄДРПОУ, до кваліфікованого надавача подається новий пакет документів відповідно до первинної процедури отримання електронних довірчих послуг, а всі чинні сертифікати ключів, виданих на цю установу, підлягають перевидачі віддалено (дистанційно) або їх скасуванню за заявкою.

У разі звільнення користувача з установи або переведення до іншої установи користувач або відповідальна особа установи звертається до кваліфікованого надавача із заявкою на скасування його кваліфікованого сертифіката, а особистий ключ знищується методом, що не допускає можливості його відновлення.

Для погодження заявок про надання кваліфікованих електронних довірчих послуг КНЕДП ЗС України може отримувати від заявників інші документи, передбачені законодавством.

Переліки, форми документів, на підставі яких надаються кваліфіковані електронні довірчі послуги, та роз’яснення щодо їх оформлення публікуються на офіційному вебсайті КНЕДП ЗС України.

До переліку суб’єктів, уповноважених подавати запит на формування кваліфікованого сертифіката, належать користувачі та/або відповідальні особи (уповноважені представники установи), що пройшли процедури ідентифікації й автентифікації відповідно до пункту 3.3.2 Політики сертифіката КНЕДП ЗС України.

Ідентифікаційні дані користувача подаються до кваліфікованого надавача або його ВПР:

- за особистої присутності користувача або відповідальної особи, якщо вона вперше звертається за отриманням послуги формування та видачі кваліфікованого сертифіката, чи в разі зміни ідентифікаційних даних, які містяться в раніше сформованому такій особі кваліфікованому сертифікаті;
- віддалено (без особистої присутності особи) шляхом надсилання через захищену систему електронного документообігу Міністерства оборони України

з накладеним на персональні дані особи, яка звертається за отриманням послуги формування та видачі кваліфікованого сертифіката, КЕП позаштатного адміністратора реєстрації, що засвідчує однозначність встановлення особи, належність підписувачу відкритого ключа та відповідного йому особистого ключа, і додатково накладеним КЕП керівника установи;

- у разі повторного дистанційного формування кваліфікованого сертифіката шляхом використання ідентифікаційних даних особи, що містяться у кваліфікованому сертифікаті, раніше сформованому та виданому за особистої присутності користувача або відповідальної особи у КНЕДП ЗС України або його ВПР.

Процес реєстрації користувача передбачає подання заявником до КНЕДП ЗС України чи його ВПР такого пакету документів:

- документ, що підтверджує повноваження користувача в установі, – підписаний керівником установи, завірений гербовою печаткою, зареєстрований установленим порядком список посадових осіб установи, довідка, яка підтверджує факт перебування на військовій службі (роботі), – форма 5 або форма 6, витяг із наказу (документ, що підтверджує повноваження користувача, дійсний протягом 30 діб від дати його реєстрації);
- картка з реєстраційними даними (заявка) встановленого зразка у двох примірниках на кожного підписувача або на електронну печатку;
- згода на обробку персональних даних КНЕДП ЗС України на кожного підписувача;
- копія паспорта громадянина України підписувача (копія 1–2 сторінки (3–6 у разі наявності відміток)) або копія паспорта підписувача, виготовлена у формі картки (далі – ID-картка), що містить безконтактний електронний носій (копії лицьової та зворотної сторін), із засвідчувальним написом та особистим підписом власника;
- копія РНОКПП із засвідчувальним написом та особистим підписом власника (якщо через релігійні переконання користувач відмовився від РНОКПП, додатково подається копія сторінки паспорта з відміткою про таку відмову, засвідчена підписом власника), а в разі якщо підписувач має паспорт у формі ID-картки, до якої внесено РНОКПП, – завірена копія РНОКПП користувачем не подається;
- запити на сертифікацію (відкриті ключі на сертифікацію) у вигляді файлів формату PKCS#10 на зареєстрованому встановленим порядком електронному носії інформації (запит на сертифікат подається у форматі відповідно до специфікації синтаксису запиту на сертифікацію), визначеному RFC 2986 “PKCS#10: Certification Request Syntax Specification”. Запит на сертифікат повинен містити інформацію про відкритий ключ, необхідні реквізити користувача, а також може містити інші ідентифікаційні дані користувача, необов’язкові додаткові спеціальні атрибути, визначені у стандартах для кваліфікованих сертифікатів, які не мають впливати на інтероперабельність і визнання кваліфікованих електронних підписів;
- завірені встановленим порядком копії інших документів, дані з яких за поданням підписувача вносяться до сертифіката.

Порядок генерації файлів запитів на сертифікацію в залежності від потреб користувача наведено в Настанові щодо порядку використання програмного забезпечення ІІТ “Користувач ЦСК-1”, що публікуються на офіційному вебсайті кваліфікованого надавача.

Документи та копії документів мають бути на білому папері формату А4 належної якості, щоб можна було прочитати увесь текст, чітко було видно всі реквізити та фото, поля документа не було порушено.

Під час розгляду картки з реєстраційними даними (заявки) на отримання кваліфікованих сертифікатів здійснюється перевірка повноти пакету поданих документів, правильність їхнього оформлення та відповідність вимогам нормативних документів у сфері електронних довірчих послуг, а також перевіряється унікальність відкритого ключа за відомостями реєстру чинних, блокованих і скасованих кваліфікованих сертифікатів. До розгляду не приймаються документи, які мають підчистки, помарки, дописки, закреслені слова, інші виправлення чи написи олівцем, а також пошкодження, внаслідок яких їхній текст неможливо прочитати.

За результатом розгляду поданих документів адміністратором реєстрації (віддаленим адміністратором реєстрації) приймається рішення про відмову в наданні кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки у випадках, якщо:

- відсутні необхідні документи, зазначені в пункті 4.1 цих Положень;
- подано хоча б одну неналежно засвідчену копію документа;
- встановлено невідповідність даних, визначених поданими документами, фактичним даним;
- виявлено інші невідповідності згідно із законодавством України.

У разі непроведення реєстрації перші примірники документів, що були надані, повертаються заявнику із відміткою адміністратора реєстрації про невідповідність, другі примірники документів залишається в кваліфікованого надавача.

Усі документи, які подаються до кваліфікованого надавача підписувачами, беруться на облік шляхом формування відповідних справ. Посадова особа КНЕДП ЗС України, на яку покладено виконання обов’язків адміністратора реєстрації (віддаленого адміністратора реєстрації) веде журнал обліку справ підписувачів, у якому зазначаються документи, на підставі яких було здійснено формування, скасування, блокування чи поновлення кваліфікованого сертифіката.

Справи користувачів зберігаються в паперовому або в електронному вигляді з урахуванням вимог законодавства у сфері архівної справи та захисту інформації в архівних приміщеннях КНЕДП ЗС України (його ВПР), доступ до яких мають лише визначені посадові особи КНЕДП ЗС України або його ВПР.

4.2. Обробка запиту на формування сертифіката

Обробка запиту на формування кваліфікованого сертифіката здійснюється програмними засобами ІКС КНЕДП ЗС України за участі адміністратора реєстрації (віддаленого адміністратора реєстрації), на якого

покладено обов’язки з реєстрації користувачів, або автоматично за умови забезпечення безперервності процесів генерації пар ключів, формування запитів, передачі їх на обробку захищеними каналами зв’язку, які забезпечують конфіденційність і цілісність даних. Автоматична обробка запитів не виключає процесів встановлення (ідентифікації) особи заявника та підтвердження володіння заявником особистим ключем, відповідний якому відкритий ключ надається для формування кваліфікованого сертифіката.

Під час обробки запиту на формування кваліфікованого сертифіката засобами ІКС КНЕДП ЗС України здійснюється перевірка відкритого ключа в реєстрі чинних, блокованих і скасованих кваліфікованих сертифікатів і забезпечується унікальність серійного номера кваліфікованого сертифіката електронного підпису чи печатки.

Розгляд поданої підписувачем або відповідальною особою картки з реєстраційними даними (заявки) на формування кваліфікованого сертифіката з відповідним пакетом документів та опрацювання запиту на сертифікат здійснюється кваліфікованим надавачем протягом робочого дня.

Строк автоматичного оброблення запиту на формування кваліфікованого сертифіката становить не більше однієї години.

4.3. Формування сертифіката

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

- шляхом запису файлу зі сформованим кваліфікованим сертифікатом на зареєстрований носій інформації, наданий підписувачем / відповідальною особою;
- шляхом публікації сформованого кваліфікованого сертифіката на електронному інформаційному ресурсі кваліфікованого надавача в разі надання згоди на публікацію до формування сертифіката;
- шляхом завантаження сертифікатів із глобальної мережі на персональному комп’ютері користувача з використанням особистого ключа підписувача за допомогою програмного забезпечення користувача КНЕДП ЗС України;
- за запитом через захищену систему електронного документообігу Міністерства оборони України.

Пункт 4.3 Політики сертифіката КНЕДП ЗС України містить додаткову інформацію.

4.4. Прийняття сертифіката

Користувач повинен протягом доби перевірити свої ідентифікаційні дані, внесені КНЕДП ЗС України або його ВПР до кваліфікованого сертифіката. Кваліфікований надавач повинен надати 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 некоректних ідентифікаційних даних,

які внесені до його кваліфікованого сертифіката, протягом доби після його отримання, користувач повинен звернутися до КНЕДП ЗС України або його ВПР із заявкою на скасування уже сформованого кваліфікованого сертифіката та карткою з реєстраційними даними (заявкою) на формування нового кваліфікованого сертифіката.

4.5. Пара ключів і призначення сертифіката

4.5.1. Використання особистого ключа та сертифіката користувачем

Використання особистого ключа користувачем здійснюється на умовах конфіденційності. Користувач зобов'язаний зберігати особистий ключ і пароль доступу до нього в таємниці та не допускати його використання іншими особами.

Користувач не має права використовувати свій особистий ключ в разі його компрометації, скасування або блокування кваліфікованого сертифіката.

Користувач зобов'язаний використовувати кваліфікований сертифікат відповідно до зазначеного в ньому призначення відкритого ключа "keyUsage" та обмеження щодо його використання.

Користувач під час використання особистого ключа та кваліфікованого сертифіката повинен дотримуватися вимог законодавства у сфері електронних довірчих послуг, вимог Регламенту КНЕДП ЗС України, Політики сертифіката КНЕДП ЗС України та цих Положень.

Для перевірки та використання особистого ключа користувач повинен мати:

- персональний комп'ютер з установленою відповідною операційною системою Microsoft Windows.
- встановлене відповідне програмне забезпечення користувача КНЕДП ЗС України, що доступне на сайті кваліфікованого надавача.

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

Суб'єкти які довіряють, перш ніж прийняти кваліфікований сертифікат користувача, зобов'язані здійснити перевірку відповідно до вимог пункту 4.5.2 Політики сертифіката КНЕДП ЗС України, а також перевірити інформацію щодо сфери використання кваліфікованого сертифіката користувача, зазначену в полі "keyUsage", та обмежень щодо його використання.

Під час використання відкритого ключа та кваліфікованого сертифіката користувача суб'єкти, які довіряють КНЕДП ЗС України, повинні дотримуватися вимог законодавства у сфері електронних довірчих послуг, вимог Регламенту КНЕДП ЗС України, Політики сертифіката КНЕДП ЗС України та цих Положень.

4.6. Поновлення сертифіката

Поновлення кваліфікованого сертифіката здійснюється у випадках, передбачених частиною десятою статті 25 Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

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

Заблокований кваліфікований сертифікат не пізніше ніж протягом двох годин поновлюється КНЕДП ЗС України в разі:

- подання користувачем заявки про поновлення його заблокованого кваліфікованого сертифіката в будь-який спосіб, що забезпечує підтвердження особи користувача (якщо блокування здійснено на підставі заявки про блокування кваліфікованого сертифіката);
- за поданням керівника установи заяви про поновлення кваліфікованого сертифіката користувача;
- повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа користувачем, уповноваженою установою або КО, який раніше повідомив про таку підозру;
- надходження до КНЕДП ЗС України повідомлення про прийняття рішення суду про поновлення кваліфікованого сертифіката, що набрало законної сили.

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

Інформація про зміну статусу кваліфікованого сертифіката на "поновлений" повідомляється адміністратором реєстрації (віддаленим адміністратором реєстрації) усно в разі його особистої присутності, а також шляхом формування та публікації кваліфікованим надавачем списків відкликаних сертифікатів і за протоколом інтерактивного визначення статусу сертифіката (OCSP).

4.7. Повторне формування сертифіката

Повторне формування кваліфікованого сертифіката здійснюється аналогічно первинній процедурі формування кваліфікованого сертифіката, за винятком того, що під час повторного звернення надається тільки картка з реєстраційними даними (заявка) (якщо внесені в сертифікат дані не змінювалися), документ, що підтверджує належність підписувача до установи, та електронні запити на формування нових кваліфікованих сертифікатів.

КНЕДП ЗС України здійснює повторне формування кваліфікованого сертифіката користувачу в один із таких способів:

- за особистої присутності фізичної особи чи відповідальної особи у КНЕДП ЗС України або його ВПР та поданими документами про повторне формування кваліфікованого сертифіката в паперовій формі;
- віддалено (дистанційно) з використанням ідентифікаційних даних особи, що містяться у кваліфікованому сертифікаті, за умови чинності такого сертифіката та відповідно до поданих документів про повторне формування кваліфікованого сертифіката.

Формування та видача нового кваліфікованого сертифіката користувачу також може здійснюватися:

- після закінчення строку дії кваліфікованого сертифіката користувача;
- у разі зміни ідентифікаційних даних користувача, яка міститься у кваліфікованому сертифікаті;
- у разі блокування ЗКЕП;

- у разі компрометації особистого ключа користувача.

При цьому, користувач повинен подати до КНЕДП ЗС України або його ВПР заявку про скасування попереднього кваліфікованого сертифіката, картку з реєстраційними даними (заявку) та пакет документів, який подається аналогічно до первинної процедури звернення.

КНЕДП ЗС України за наявності технічної можливості може повторно сформувати кваліфікований сертифікат підписувачу чи створювачу електронної печатки, який є власником чинного кваліфікованого сертифіката, сформованого кваліфікованим надавачем. Формування здійснюється на підставі електронного запиту на формування нового кваліфікованого сертифіката з накладанням кваліфікованого електронного підпису чи печатки, що відповідає чинному на момент підписання кваліфікованому сертифікату підписувача чи створювача електронної печатки. Таким чином 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, попередній сертифікат скасовується.

4.8. Зміна сертифіката

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

4.9. Блокування та скасування сертифіката

Кваліфікований сертифікат скасовується КНЕДП ЗС України або його ВПР протягом двох годин у разі:

- подання користувачем заявки на скасування виданого йому кваліфікованого сертифіката в будь-який спосіб, що забезпечує підтвердження особи користувача;
- подання заявки на скасування кваліфікованого сертифіката посадової чи юридичної особи за підписом відповідальної особи;
- надходження до КНЕДП ЗС України інформації, що підтверджує:

смерть фізичної особи – користувача;

державну реєстрацію припинення юридичної особи;

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, яка є підписувачем, якій видано кваліфікований сертифікат автентифікації вебсайту або яка є створювачем електронної печатки, померлою, визнання її безвісно відсутньою, недієздатною,

обмеження її цивільної дієздатності.

Користувач може самостійно здійснити скасування власного кваліфікованого сертифіката за електронним запитом, що не потребує оформлення паперових документів.

Дана процедура підтримується цілодобово за допомогою програмного забезпечення ІІТ “Користувач ЦСК-1” та особистого ключа підписувача.

Процедуру самостійного скасування власного кваліфікованого сертифіката за електронним запитом наведено в Настанові щодо порядку використання програмного забезпечення ІІТ “Користувач ЦСК-1”.

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

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 ЗС України, якщо протягом зазначеного строку користувач не поновить його чинність.

КНЕДП ЗС України блокує сформований ним кваліфікований сертифікат не пізніше ніж протягом двох годин у разі:

- подання користувачем заявки на блокування виданого йому кваліфікованого сертифіката в будь-який спосіб, що забезпечує підтвердження особи користувача;
- подання заявки на блокування кваліфікованого сертифіката юридичної особи за підписом відповідальної особи (уповноваженого представника установи);
- повідомлення (подання) користувачем, відповідальною особою установи, представником уповноваженої установи Міністерства оборони України та/або ЗС України або КО про підозру в компрометації особистого ключа користувача;
- набрання законної сили рішенням суду про блокування кваліфікованого сертифіката.

Користувач може здійснити блокування кваліфікованого сертифіката в телефонному режимі. Заявка в усній формі подається до КНЕДП ЗС України засобами телефонного зв’язку за номерами +38(044)454-41-06, (62)2-32-06, при цьому користувач повинен повідомити адміністратору реєстрації таку інформацію:

ідентифікаційні дані власника кваліфікованого сертифіката;

ключову фразу голосової автентифікації.

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

Користувач може самостійно здійснити блокування власного кваліфікованого сертифіката за електронним запитом, що не потребує оформлення паперових документів.

Дана процедура підтримується цілодобово за допомогою програмного забезпечення ІІТ “Користувач ЦСК-1” та особистого ключа підписувача.

Процедуру самостійного блокування власного кваліфікованого сертифіката за електронним запитом наведено в Настанові щодо порядку використання програмного забезпечення ІІТ “Користувач ЦСК-1”.

Перелік підстав для зміни статусу кваліфікованого сертифіката на “блокований” і “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” і “скасований”

Підстави для зміни статусу сертифіката	**Скасування**	**Блокування**	**Підтвердження підстав**
Подання користувачем заяви	+	+	Заявка користувача
Смерть фізичної особи – користувача	+		Документальне підтвердження
Припинення діяльності користувача (фізичної або юридичної особи)	+		Документальне підтвердження
Зміни ідентифікаційних даних користувача	+		Документальне підтвердження
Надання користувачем недостовірних ідентифікаційних даних	+		Документальне підтвердження
Факт компрометації особистого ключа користувача, виявлений самостійно користувачем або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг	+		Заявка користувача або документальне підтвердження
Повідомлення користувачем, представником уповноваженої установи або КО про підозру в компрометації особистого ключа користувача електронних довірчих послуг		+	Заявка користувача або документальне підтвердження
Набрання законної сили рішенням суду	+	+	Документальне підтвердження

КНЕДП ЗС України або його ВПР встановлює (ідентифікує) особу, яка звертається із заявкою на скасування або блокування кваліфікованого сертифіката, а також перевіряє законність такого звернення.

КНЕДП ЗС України здійснює цілодобовий прийом і перевірку заявок підписувачів і створювачів електронних печаток про скасування та блокування їх кваліфікованих сертифікатів із використанням інформаційних каналів, відомості про які наведено на офіційному сайті КНЕДП ЗС України.

Кваліфіковані сертифікати скасовуються, блокуються та поновлюються КНЕДП ЗС України не пізніше ніж протягом двох годин із моменту отримання заявок від фізичних осіб або відповідальних осіб, підтвердження підстав для зміни статусу сертифіката та здійснення відповідної перевірки достовірності документальних повідомлень та автентифікації заявників.

Інформація про зміну статусу кваліфікованого сертифіката на “скасований” або “блокований” розповсюджується шляхом формування та публікації КНЕДП ЗС України списків відкликаних сертифікатів і за протоколом інтерактивного визначення статусу сертифіката (OCSP).

4.10. Послуга перевірки статусу сертифіката

КНЕДП ЗС України забезпечує підтримку сервісу перевірки статусу сертифіката в режимі реального часу за допомогою OCSP-сервера та списків відкликаних сертифікатів (CRL), що публікуються на вебсайті кваліфікованого надавача.

Інформація про статус кваліфікованого сертифіката користувача доступна цілодобово.

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 закінчення строку дії сертифіката користувача, зазначеного в ньому, такий сертифікат вважається скасованим.

4.12. Депонування та повернення ключів

Не застосовується.

5. ОБ’ЄКТ, УПРАВЛІННЯ Й ОПЕРАЦІЙНИЙ КОНТРОЛЬ

До об’єктів, процесів і заходів, зазначених у 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 КНЕДП ЗС України містить інформацію щодо вимог до приміщень КНЕДП ЗС України та забезпечення фізичного доступу до них.

5.2. Процедурний контроль

Пункт 5.2 та пункт 5.3.1 Політики сертифіката КНЕДП ЗС України містять інформацію щодо процедурного контролю та інформацію щодо довірених ролей персоналу КНЕДП ЗС України (керівник, адміністратор реєстрації, адміністратор сертифікації, адміністратор безпеки, системний адміністратор, аудитор системи) та їхніх функціональних обов’язків, щодо кількості осіб, необхідних для виконання завдань, а також довірених ролей персоналу КНЕДП ЗС України, що вимагають розподілу обов’язків.

5.3. Контроль персоналу

Пункт 5.3 Політики сертифіката КНЕДП ЗС України містить інформацію щодо вимог до кваліфікації, досвіду та допуску персоналу КНЕДП ЗС України, вимог і процедур навчання, контролю відокремлених пунктів реєстрації КНЕДП ЗС України, документації, яка надається персоналу КНЕДП ЗС України.

5.4. Ведення журналу аудиту подій

Пункт 5.4 Політики сертифіката КНЕДП ЗС України 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 і питань синхронізації часу.

5.5. Архів документів

Пункт 5.5 Політики сертифіката КНЕДП ЗС України містить інформацію щодо видів документів і 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 КНЕДП ЗС України містить інформацію щодо підстав і періодичності зміни пари ключів КНЕДП ЗС України, порядку використання та доступу до актуального відкритого ключа КНЕДП ЗС України.

5.7. Компрометація й аварійне відновлення

Пункт 5.7 Політики сертифіката КНЕДП ЗС України 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 безперервної роботи після катастрофи.

5.8. Припинення діяльності кваліфікованого надавача

Пункт 5.8 Політики сертифіката КНЕДП ЗС України містить інформацію щодо підстав припинення діяльності КНЕДП ЗС України, 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 ЗС України.

6. ТЕХНІЧНІ ЗАХОДИ БЕЗПЕКИ

До об’єктів, процесів і заходів, зазначених у 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 КНЕДП ЗС України містить інформацію щодо генерації пари ключів КНЕДП ЗС України та користувачів, доставки особистого та відкритого ключів користувачам, доставки відкритого ключа КНЕДП ЗС України суб’єктам, які довіряють КНЕДП ЗС України, щодо розмірів ключів, генерації параметрів відкритого ключа КНЕДП ЗС України та перевірки якості, основних цілей використання особистих ключів КНЕДП

ЗС України.

6.2. Захист особистого ключа та інженерний контроль криптографічного модуля

Пункт 6.2 Політики сертифіката КНЕДП ЗС України 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 мережевого криптографічного модуля.

6.3. Інші аспекти керування парами ключів

Пункт 6.3 Політики сертифіката КНЕДП ЗС України містить інформацію щодо архівації відкритого ключа КНЕДП ЗС України, строків дії сертифіката та строків використання пари ключів КНЕДП ЗС України.

6.4. Дані активації

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

6.5. Контроль комп'ютерної безпеки

Пункт 6.5 Політики сертифіката КНЕДП ЗС України 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 КНЕДП ЗС України містить інформацію щодо контролю розробки ІКС КНЕДП ЗС України, засобів керування безпекою в ІКС КНЕДП ЗС України, контролю безпеки протягом життєвого циклу.

6.7. Контроль безпеки мережі

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

6.8. Електронні позначки часу

Пункт 6.8 Політики сертифіката КНЕДП ЗС України містить інформацію щодо формування та перевірки кваліфікованої електронної позначки часу, наслідків недійсності кваліфікованої електронної позначки часу та процедури отримання КНЕДП ЗС України кваліфікованої електронної позначки часу.

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

До об'єктів, процесів і заходів, зазначених у 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 КНЕДП ЗС України містить інформацію щодо відомостей, які повинні міститися у кваліфікованих сертифікатах.

7.2. Профілі списку відкликаних сертифікатів

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

7.3. Профілі протоколу визначення статусу сертифіката

Пункт 7.3 Політики сертифіката КНЕДП ЗС України містить інформацію щодо можливості перевірки статусу кваліфікованого сертифіката користувача в режимі реального часу через електронні комунікаційні мережі загального користування з використанням протоколу OCSP.

8. АУДИТ ВІДПОВІДНОСТІ ТА ІНШІ ОЦІНКИ

До об’єктів, процесів і заходів, зазначених у 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 й обставини оцінювання

Пункт 8.1 Політики сертифіката КНЕДП ЗС України містить інформацію щодо частоти й обставин здійснення КО державного нагляду (контролю) за дотриманням КНЕДП ЗС України вимог законодавства у сфері електронних довірчих послуг.

8.2. Особа / кваліфікація оцінювача

Пункт 8.2 Політики сертифіката КНЕДП ЗС України містить інформацію щодо вимог до кваліфікації посадових осіб КО й органу з оцінки відповідності ООВ та організації, що проводить аудит системи захисту інформації.

8.3. Відносини експерта з об’єктом оцінки

Пункт 8.3 Політики сертифіката КНЕДП ЗС України містить інформацію щодо відносин посадових осіб КО й експертів (аудиторів) органу з оцінки відповідності з об’єктом оцінки (КНЕДП ЗС України) й експертів, що проводять аудит системи захисту інформації.

8.4. Теми, охоплені оцінюванням

Пункт 8.4 Політики сертифіката КНЕДП ЗС України містить інформацію щодо питань, які підлягають перевірці під час державного контролю, під час оцінки відповідності та під час аудиту системи захисту інформації.

8.5. Дії, вжиті внаслідок порушення

Пункт 8.5 Політики сертифіката КНЕДП ЗС України містить інформацію щодо дій, які вживаються внаслідок порушення, виявленого за результатами державного контролю, за результатами оцінки відповідності та за результатами аудиту системи захисту інформації.

8.6. Повідомлення результатів

Пункт 8.6 Політики сертифіката КНЕДП ЗС України містить інформацію щодо оформлення результатів державного контролю, надання припису про усунення порушень, виявлених під час державного контролю, оцінки відповідності та аудиту системи захисту інформації.

8.7. Самоперевірки

Пункт 8.7 Політики сертифіката КНЕДП ЗС України містить інформацію щодо проведення кваліфікованим надавачем регулярних внутрішніх аудитів дотримання встановлених вимог.

9. ІНШІ КОМЕРЦІЙНІ ТА ЮРИДИЧНІ ПИТАННЯ

До об’єктів, процесів і заходів, зазначених у 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 й тарифи

9.1.1. Плата за видачу або поновлення сертифіката

Формування кваліфікованого сертифіката для користувачів (працівників) установ, що відносяться до сфери управління Міністерства оборони України та/або підпорядковані (придані) військовому командуванню Збройних Сил України, здійснюється КНЕДП ЗС України на безоплатній основі.

Поновлення заблокованих кваліфікованих сертифікатів здійснюється КНЕДП ЗС України на безоплатній основі.

9.1.2. Плата за доступ до сертифіката

Доступ для користувачів (працівників) установ, що відносяться до сфери управління Міністерства оборони України та/або підпорядковані (придані) військовому командуванню Збройних Сил України, до кваліфікованих сертифікатів є безкоштовним.

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

Блокування, скасування, а також доступ до інформації про статус кваліфікованого сертифіката для користувачів (працівників) установ, що відносяться до сфери управління Міністерства оборони України та/або підпорядковані (придані) військовому командуванню Збройних Сил України, є безкоштовним.

9.1.4. Плата за інші послуги

Для користувачів (працівників) установ, що відносяться до сфери управління Міністерства оборони України та/або підпорядковані (придані) військовому командуванню Збройних Сил України, послуги надаються на безоплатній основі.

Апаратно-програмні або апаратні засоби кваліфікованого електронного підпису установи отримують через служби забезпечення інформаційно-комунікаційних систем, у яких ці засоби застосовуються, або організовують закупівлю ЗКЕП.

9.1.5. Політика відшкодування

КНЕДП ЗС України не відшкодовує рахунки на послуги, що були надані на безоплатній основі.

9.2. Фінансова відповідальність

Пункт 9.2 Політики сертифіката КНЕДП ЗС України містить інформацію щодо страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути завдана КНЕДП ЗС України користувачам чи третім особам.

9.3. Конфіденційність ділових даних

Пункти 9.3. та 9.4 Політики сертифіката КНЕДП ЗС України містить відомості про конфіденційну інформацію, яка обробляється в ІКС КНЕДП ЗС України, інформацію, яка не належить до конфіденційної, а також про відповідальність за порушення конфіденційності ділової інформації.

9.4. Захист персональних даних

Пункт 9.5 Політики сертифіката КНЕДП ЗС України містить інформацію

щодо порядку захисту персональних даних в КНЕДП ЗС України.

9.5. Права інтелектуальної власності

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

9.6. Заяви та гарантії

Пункт 9.7 Політики сертифіката КНЕДП ЗС України містить інформацію щодо зобов'язань і гарантій КНЕДП ЗС України, ВПР КНЕДП ЗС України, користувачів, суб'єктів, які довіряють кваліфікованому надавачу, а також інших учасників.

9.7. Відмова від відповідальності

Пункт 9.8 Політики сертифіката КНЕДП ЗС України містить інформацію щодо відмови від гарантій КНЕДП ЗС України.

9.8. Обмеження відповідальності

Пункт 9.9 Політики сертифіката КНЕДП ЗС України містить інформацію щодо обставин для обмеження відповідальності кваліфікованого надавача.

9.9. Відшкодування збитків

Відшкодування збитків, які можуть бути завдані користувачам електронних довірчих послуг чи третім особам внаслідок неналежного виконання КНЕДП ЗС України своїх зобов'язань, здійснюється відповідно до вимог чинного законодавства України.

9.10. Термін дії та припинення дії

Регламент роботи КНЕДП ЗС України та, зокрема, ці Положення діють із моменту їх затвердження та опублікування на вебсайті КНЕДП ЗС України до закінчення строку дії останнього сертифіката, виданого відповідно до цих Положень або до моменту припинення діяльності КНЕДП ЗС України.

9.11. Індивідуальні повідомлення та комунікації з учасниками інфраструктури відкритих ключів

КНЕДП ЗС України здійснює комунікацію з учасниками інфраструктури відкритих ключів шляхом:

- розміщення повідомлень та оголошень на вебсайті КНЕДП ЗС України;
- засобами телефонного зв'язку, що зазначені підписувачем або відповідальною особою в картці з реєстраційними даними (заявці);
- інформування ЦЗО, КО й органу з питань захисту персональних даних шляхом надсилання повідомлень у паперовій та електронній формах;
- доведення повідомлень та оголошень, що містять інформацію з обмеженим доступом, до учасників інфраструктури відкритих ключів в установленому законодавством порядку.

9.12. Зміни

Внесення змін і доповнень до цих Положень здійснюється в разі:

- змін вимог, процесів і процедур, описаних у цих Положеннях;
- змін у законодавстві;
- змін у вимогах до надавачів щодо надання послуг.

Нові версії цих Положень публікуються на вебсайті КНЕДП ЗС України.

Будь-які зміни, не зазначені в історії цих Положень, є граматичними

й орфографічними змінами, які не впливають на суть і не стосуються процесів і процедур, описаних у цих Положеннях.

9.13. Порядок вирішення спорів

У випадку виникнення спорів або розбіжностей КНЕДП ЗС України вирішує їх шляхом переговорів і консультацій з учасниками інфраструктури відкритих ключів.

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

9.14. Застосовне право

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

9.15. Дотримання чинного законодавства

Під час надання кваліфікованих електронних довірчих послуг КНЕДП ЗС України повинен дотримуватись вимог законодавства у сферах електронних довірчих послуг, технічного та криптографічного захисту інформації, захисту персональних даних.

Перелік відповідних нормативно-правових актів зазначено в пункті 9.16 Політики сертифіката КНЕДП ЗС України та не є вичерпним.

Командир військової частини А0136
полковник — Віталій КІНЧЕВСЬКИЙ