



НАКАЗ

ГОЛОВНОКОМАНДУВАЧА ЗБРОЙНИХ СИЛ УКРАЇНИ

15.01.2021

м. Київ

№ 11

Про затвердження Порядку
отримання електронних
довірчих послуг у Збройних
Силах України

Відповідно до Закону України “Про електронні довірчі послуги”, постанови Кабінету Міністрів України від 19 вересня 2018 року № 749 “Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності”, Регламенту роботи кваліфікованого надавача електронних довірчих послуг “Центр сертифікації ключів Збройних Сил України”, з метою отримання і використання електронних довірчих послуг, які надає кваліфікований надавач електронних довірчих послуг “Центр сертифікації ключів Збройних Сил України” для виконання посадових (службових) обов’язків, **н а к а з у ю**:

1. Затвердити Порядок отримання електронних довірчих послуг у Збройних Силах України, що додається.

2. Визнати таким, що втратив чинність, наказ Генерального штабу Збройних Сил України від 30 травня 2019 року № 200 “Про затвердження Порядку отримання електронних довірчих послуг у Збройних Силах України”.

3. Наказ розіслати згідно з розрахунком розсилки.

Головнокомандувач Збройних Сил України
генерал-полковник



Руслан ХОМЧАК

ЗАТВЕРДЖЕНО

Наказ Головнокомандувача
Збройних Сил України
15 січня 2021 року № 11

ПОРЯДОК
отримання електронних довірчих послуг
у Збройних Силах України

1. Загальні положення

1.1. Цей Порядок встановлює вимоги щодо отримання кваліфікованих електронних довірчих послуг, їх застосування підписувачами та установами у Збройних Силах України.

1.2. Порядок отримання та застосування кваліфікованих електронних довірчих послуг для технічних та/або програмних засобів, обслуговуючого персоналу, а також мережевих ресурсів (поштових серверів, вебсайтів тощо) визначається діючим Порядком надання електронних довірчих послуг для інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем Міністерства оборони України та Збройних Сил України та інструкціями зі складу документації комплексних систем захисту інформації в системах, затверджених в установленому порядку.

1.3. У цьому Порядку терміни вживаються у такому значенні:

відкритий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;

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

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

доменне ім'я (домен) – символічне позначення для адресації вузлів мережі та мережевих ресурсів (вебсайтів, серверів електронної пошти, мережевих серверів, тощо) в зручній для людини формі.

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

захищений носій особистих ключів – засіб кваліфікованого електронного підпису чи печатки, призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на ньому даних від несанкціонованого доступу, безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання;

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

ідентифікація особи – процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи;

кваліфікований сертифікат відкритого ключа (далі – сертифікат 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 та можуть розповсюджуватись у формі документа на папері;

користувачі електронних довірчих послуг (далі – користувачі) – заявники, підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних, інші фізичні та юридичні особи, які отримують кваліфіковані електронні довірчі послуги у надавачів таких послуг;

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

пара ключів – особистий та відповідний йому відкритий ключі, що є взаємопов'язаними параметрами алгоритму асиметричного криптографічного перетворення;

посадові особи – це військовослужбовці, державні службовці та працівники установ, які виконують організаційно-розпорядчі або адміністративно-господарські функції;

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

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

розпорядник вебсайту – установа, якій володільцем вебсайту або вищим органом військового управління поставлено завдання ведення (супроводження) вебсайту, забезпечення роботи вебсерверу або здійснення адміністративного супроводу домену (доменного ім'я вебсайту);

установа – структурний підрозділ апарату Міністерства оборони України, Апарату Головнокомандувача Збройних Сил України, Генерального штабу Збройних Сил України та безпосередньо їм підпорядковані структурні підрозділи, командування видів, окремих родів військ (сил) Збройних Сил України, оперативних командувань, військових частин, установ та організацій, інший постійно чи тимчасово утворений орган для управління військами (силами), військовий комісаріат.

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

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

1.4. Посадові особи установ для виконання своїх посадових (службових) обов’язків отримують електронні довірчі послуги у кваліфікованого надавача електронних довірчих послуг Збройних Сил України “Центр сертифікації ключів Збройних Сил України” (далі – кваліфікований надавач) та його відокремлених пунктах реєстрації (далі – ВПР).

Для здійснення цивільно-правових відносин у державних інформаційних системах, ці особи можуть звернутися у встановленому порядку до кваліфікованого надавача чи його ВПР з метою отримання додаткового кваліфікованого електронного підпису фізичної особи.

1.5. Ідентифікаційні дані кваліфікованого надавача

Повне найменування: кваліфікований надавач електронних довірчих послуг “Центр сертифікації ключів Збройних Сил України”

Місцезнаходження кваліфікованого надавача: 03168, м. Київ, просп. Повітрофлотський, 6.

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

Електронна адреса інформаційного ресурсу (вебсайту):

мережі “Інтернет” – <http://ca.mil.gov.ua>

інформаційно-телекомунікаційної мережі автоматизованої системи управління Збройних Сил України “Дніпро”: <http://172.16.1.48:80>.

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

1.6. Функції кваліфікованого надавача виконує структурний підрозділ військової частини А0136. Юридична адреса військової частини А0136: 03022, м. Київ, вул. Михайла Максимовича, 3.

1.7. Реалізацію функцій кваліфікованого надавача з реєстрації підписувачів та їх обслуговування на визначеній території здійснюють ВПР, які є територіально відокремленими підрозділами кваліфікованого надавача без правового статусу юридичної особи.

Ідентифікаційні дані ВПР розміщені на інформаційному ресурсі кваліфікованого надавача.

Персонал, що забезпечує роботу ВПР, підпорядковується керівнику кваліфікованого надавача з питань надання електронних довірчих послуг.

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

1.8. Функції позаштатного адміністратора реєстрації в установі виконує керівник кадрового органу.

1.9. Форми документів, необхідних для отримання, скасування, блокування, поновлення кваліфікованих сертифікатів відкритих ключів посадових осіб та електронної печатки, розроблені керівником кваліфікованого надавача та опубліковані на електронному інформаційному ресурсі кваліфікованого надавача.

1.10. Порядок отримання електронних довірчих послуг, форми документів, необхідних для отримання електронних довірчих послуг для технічних та/або програмних засобів та обслуговуючого персоналу в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах військового призначення (далі – ІТС), визначаються інструкціями зі складу документації комплексної системи захисту інформації в цих системах. Вимоги цих інструкцій повинні враховувати технічні можливості програмно-технічного комплексу та положення Регламенту роботи кваліфікованого надавача електронних довірчих послуг “Центр сертифікації ключів Збройних Сил України” (далі – Регламент). Такі інструкції опрацьовують розробники або власники (розпорядники) комплексної системи захисту інформації в цих ІТС та обов’язково погоджують їх з керівником кваліфікованого надавача.

Власник ІТС для забезпечення отримання електронних довірчих послуг від кваліфікованого надавача надсилає на адресу військової частини А0136 заявку про надання електронних довірчих послуг, завірені встановленим порядком копії (або витяг) інструкції та завірену копію атестату відповідності на комплексну систему захисту інформації в ІТС.

1.11. Електронна взаємодія підписувачів та створювачів електронних печаток, яка потребує відправлення, отримання, використання та постійного зберігання за участю третіх осіб електронних даних, аналоги яких на

паперових носіях повинні містити власноручний підпис відповідно до законодавства, а також автентифікація в складових частинах інформаційних систем, в яких здійснюється обробка таких електронних даних та володільцями інформації в яких є органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, повинні здійснюватися з використанням кваліфікованих електронних довірчих послуг.

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

1.12. Для зберігання особистого ключа удосконаленого електронного підпису, який базується на кваліфікованому сертифікаті відкритого ключа можуть використовувати електронні носії інформації (далі – ЕНІ)¹, при цьому генерується тільки ключ електронного підпису без використання окремого ключа протоколу розподілу ключів (надається відповідно до постанови Кабінету Міністрів України від 03.03.2020 № 193 “Про реалізацію експериментального проекту щодо забезпечення можливості використання удосконалених електронних підписів і печаток, які базуються на кваліфікованих сертифікатах відкритих ключів”).

1.13. Для визначення достовірності походження та проведення перевірки цілісності електронних даних, а також ідентифікації державної установи як підписувача, у тому числі для засвідчення відповідності електронних копій електронних та паперових (фотокопія) документів оригіналу у випадках, передбачених законодавством, установа застосовує кваліфіковану електронну печатку. При цьому кваліфікована електронна печатка створюється за допомогою захищених носіїв особистих ключів.

Перелік електронних документів, які потребують засвідчення електронною печаткою, визначається інструкцією з діловодства установи.

Рішенням керівника установи визначається необхідність використання кваліфікованої електронної печатки та уповноважені посадові особи, відповідальні за її застосування.

1.14. Кваліфікована електронна печатка видається на найменування установи, зазначеному в довідці з ЄДРПОУ.

¹ USB-flash носій, CD-R(RW), DVD-R(RW), HDD, тощо.

Особистий ключ електронної печатки формується виключно на захищеному носії особистого ключа в апаратному режимі, при цьому генерується тільки ключ електронного підпису без використання окремого ключа протоколу розподілу ключів.

1.15. Генерація особистого та відкритого ключів здійснюється особисто заявником, підписувачем та/або створювачем електронної печатки відповідно до пункту 4.14.3 розділу 4 Регламенту.

Регламент розміщений на електронному інформаційному ресурсі (вебсайт кваліфікованого надавача).

Генерація пари ключів здійснюється виключно на носій, який видано підписувачу (формувачу електронної печатки) в користування:

на виданому за накладною або іншим способом захищеному носії особистого ключа для зберігання кваліфікованого електронного підпису чи печатки;

на виданому електронному носії інформації, що зареєстрований в нетаємному службовому діловодстві установи з позначкою /ЕП, наприклад: інв. № 111/ЕП для зберігання удосконаленого електронного підпису, що базується на кваліфікованому сертифікаті відкритого ключа.

Після генерації підписувачем пари ключів особистий ключ залишається у нього, а відкритий (запит на сертифікацію) передається на сертифікацію відповідно до пункту 4.16 Регламенту.

Підписувач несе особисту відповідальність за забезпечення конфіденційності та цілісності особистого ключа.

2. Використання кваліфікованого електронного підпису в установі

2.1. Відповідальність за організацію отримання та використання кваліфікованих електронних довірчих послуг в установі несе її керівник.

2.2. Організацію використання кваліфікованих електронних довірчих послуг в установі забезпечує відповідальний підрозділ, що виконує відповідні функції, або відповідальні особи, визначені наказом керівника цієї установи. Відповідальний підрозділ (відповідальні особи) забезпечує:

підготовку та подання кваліфікованому надавачу інформації, необхідної для отримання кваліфікованих електронних довірчих послуг;

підготовку та подання кваліфікованому надавачу інформації, необхідної для отримання кваліфікованих електронних довірчих послуг;

надання допомоги підписувачам під час генерації їх особистих та відкритих ключів;

ознайомлення підписувачів з правилами застосування кваліфікованих електронних довірчих послуг та здійснення контролю за їх дотриманням;

взаємодію з кваліфікованим надавачем з питань використання кваліфікованих електронних довірчих послуг;

подання кваліфікованому надавачу заяв про скасування, блокування або поновлення кваліфікованих сертифікатів відкритих ключів;

ведення обліку захищених носіїв особистих ключів та засобів кваліфікованого електронного підпису чи печатки;

зберігання оригіналів документів та/або їх копій (крім копій особистих документів підписувачів, що містять їх персональні дані), на підставі яких отримано кваліфіковані електронні довірчі послуги;

здійснення контролю за використанням підписувачами засобів кваліфікованого електронного підпису чи печатки та зберіганням ними особистих ключів.

2.3. Керівник установи організовує ознайомлення підписувачів, які будуть застосовувати електронні довірчі послуги у повсякденній діяльності, з вимогами Регламенту та нормативно-правовими актами України у сфері електронних довірчих послуг, розміщеними на електронному інформаційному ресурсі кваліфікованого надавача.

2.4 Ідентифікація особи під час формування та видачі кваліфікованого сертифіката відкритого ключа

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

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

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

3. Документи, необхідні для реєстрації заявників та підписувачів

3.1. Установи отримують від кваліфікованого надавача або його ВПР електронні довірчі послуги за заявками керівників установ, які надсилаються до службового діловодства військової частини А0136.

Разом із заявкою надсилаються:

копія довідки про внесення установи (юридичної особи) до ЄДРПОУ, засвідчена в установленому порядку;

витяг з наказу або звірена в установленому порядку копія наказу керівника установи про призначення відповідальної особи за організацію використання кваліфікованих електронних довірчих послуг в установі (пункт 2.2 Порядку).

У разі зміни відповідальних осіб вносяться зміни до існуючого наказу або видається новий наказ із зазначенням, що попередній втратив чинність. Витяг з наказу або звірена в установленому порядку копія наказу надсилається до службового діловодства військової частини А0136 та ВПР, у якому обслуговується установа, разом із супровідним листом.

Заявки установ, які будуть отримувати електронні довірчі послуги у його ВПР, розглядаються керівником кваліфікованого надавача, копії з резолюцією надсилаються до ВПР для їх відпрацювання.

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

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

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

На підставі наданих підписувачем/відповідальною особою документів, що підтверджують зміни відомостей, які містяться у кваліфікованому сертифікаті електронного підпису підписувача, надавач здійснює скасування сертифіката та формування нового відповідно до пунктів 4.5 – 4.6 Регламенту.

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

У разі звільнення підписувача з установи або переведення до іншої установи підписувач або відповідальна особа установа звертаються до кваліфікованого надавача для скасування його кваліфікованого сертифіката відкритого ключа із заявкою, а особистий ключ знищується методом, що не допускає можливості його відновлення.

3.2. Як правило, ідентифікаційними даними, які заносяться до кваліфікованого сертифіката підписувача, є:

прізвище, ім'я та по батькові підписувача;
реєстраційний номер облікової картки платника податків (РНОКПП)²;
найменування установи згідно з ЄДРПОУ;
код установи згідно з ЄДРПОУ;
місце реєстрації установи за Державним класифікатором об'єктів адміністративно-територіального устрою України (місце знаходження згідно з ДКОАТУУ).

3.3. До кваліфікованих сертифікатів відкритих ключів можуть вноситися додаткові дані (поля) (додаток 1), що відповідають вимогам міжнародного стандарту RFC 5280 збірки стандартів X.509, а також враховують вимоги Регламенту та політики сертифікації кваліфікованого надавача.

Додаткові дані, які вносяться до кваліфікованих сертифікатів відкритих ключів підписувачів, повинні бути підтверджені відповідними документами та внесені до реєстраційної картки. До додаткових даних належать: підрозділ, посада, унікальний номер запису в Єдиному державному демографічному реєстрі (УНЗР), телефон, поштова адреса тощо (додаток 1).

3.4. Вносити до кваліфікованих сертифікатів інформацію з обмеженим доступом категорично забороняється.

3.5. Документи, необхідні для отримання електронних довірчих послуг: документ, що підтверджує належність підписувача до установи – підписаний керівником установи, завірений гербовою печаткою та з кутовим штампом установи: список посадових осіб установи, яким необхідно отримати кваліфіковані електронні довірчі послуги або форма 5 для військовослужбовців, форма 6 для працівників Збройних Сил України та державних службовців на кожного підписувача;

реєстраційна картка встановленого зразка у двох примірниках на кожного підписувача або на електронну печатку;

згода на обробку персональних даних кваліфікованим надавачем на кожного підписувача;

копія паспорта громадянина України підписувача (копії 1-2 сторінок (3-6 за наявності відміток) або копія паспорта підписувача, виготовленого у формі картки, що містить безконтактний електронний носій (копії лицьової та зворотної сторін), засвідчені підписом власника;

копія картки платника податків, засвідчена підписом власника, або копія сторінки паспорта з відміткою про відмову від прийняття реєстраційного номера облікової картки платника податків через релігійні переконання³;

2 - у разі, якщо через релігійні переконання посадова особа відмовилась від РНОКПП, до кваліфікованого надавача подається копія сторінки паспорта з відповідною відміткою.

3- у разі наявності в паспорті посадової особи запису про відмову від ідентифікаційного коду через релігійні переконання, копія облікової картки платника податків не подається.

копії інших документів, дані з яких вносяться до сертифіката;
відкриті ключі на сертифікацію (запити на сертифікацію) у вигляді файлів формату PKCS#10 на зареєстрованому ЕНІ.

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

Документи, наведені в п. 3.5. Порядку, надаються кваліфікованому надавачу заявником, підписувачем, створювачем електронної печатки або відповідальною особою окремо від заявки.

3.7. Повторне формування кваліфікованого сертифіката відкритого ключа здійснюється відповідно до первинної процедури формування кваліфікованого сертифіката відкритого ключа. У разі повторного звернення надається тільки картка з реєстраційними даними (якщо дані, які внесені до сертифіката не змінювалися), документ, що підтверджує належність підписувача до установи, та надається електронний запит на формування нового кваліфікованого сертифіката відкритого ключа.

3.8. У разі необхідності відображення в кваліфікованому сертифікаті ключа за міжнародними алгоритмами підписувача прізвища та ім'я або інших даних латиницею, дані в реєстраційну картку вносяться із закордонного паспорта підписувача або іншого документа, який унеможливорює виникнення будь-яких сумнівів щодо особи та правильного написання її ідентифікаційних даних латиницею.

4. Облік, зберігання, скасування, блокування, поновлення та знищення особистих ключів підписувачів установи

4.1. Облік особистих ключів кваліфікованого електронного підпису здійснюється шляхом реєстрації носія особистого ключа в журналі обліку та видачі ключових даних кваліфікованого електронного підпису (далі – Журнал) (додаток 2). Облік та видачу особистих ключів установи здійснює відповідальна особа.

4.2. Носій особистого ключа кваліфікованого електронного підпису або печатки повинен зберігатися таким способом, який унеможливорює доступ до нього сторонніх осіб.

Передача особистих ключів кваліфікованого електронного підпису стороннім особам категорично забороняється.

У разі передачі носія з особистим ключем електронного підпису та пароля до нього сторонній особі ключ вважається скомпрометованим, сертифікат його відкритого ключа підлягає негайному блокуванню та подальшому скасуванню.

4.3. Скасування, блокування та поновлення кваліфікованих сертифікатів відкритих ключів здійснюється відповідно до п. 5.6 Регламенту.

4.4. Знищення особистого ключа здійснюється методом, що не допускає можливості відновлення особистого ключа:

з використанням особистого ключа підписувача за допомогою програмного забезпечення ІТ "Користувач ЦСК-1". Настанова щодо порядку використання програмного забезпечення ІТ "Користувач ЦСК-1" розміщена на інформаційному ресурсі кваліфікованого надавача;

методом стирання ключа з ЕНІ – методом форматування;

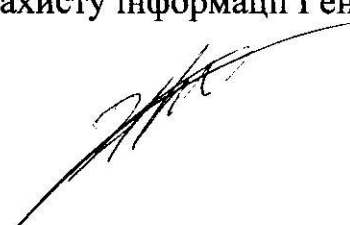
методом знищення самого ЕНІ – за допомогою технічних засобів, що унеможлиблює його відновлення.

Знищення особистого ключа фіксується відповідальною особою в Журналі.

4.5. У разі звільнення підписувача з установи або переведення до іншої установи підписувач зобов'язаний повернути виданий йому для користування захищений носій особистого ключа в підрозділ забезпечення установи.

Тимчасово виконуючий обов'язки начальника Центрального управління охорони державної таємниці та захисту інформації Генерального штабу Збройних Сил України

полковник



Ігор БОЙКО

Додаток 1

до Порядку отримання
електронних довірчих послуг у
Збройних Силах України
(пункт 3.3.)

РЕЄСТРАЦІЙНІ ДАНІ

які можуть бути внесені до реєстраційної картки
на отримання кваліфікованих сертифікатів відкритих ключів посадових осіб
та електронної печатки

Обов'язкові поля

Назва поля	Тип даних поля	Об'єм даних поля
Найменування	текстове	до 64 знаків включаючи пробіли
Установа	текстове	до 64 знаків включаючи пробіли

Необов'язкові поля

Назва поля	Тип даних поля	Об'єм даних поля
Підрозділ	текстове	до 64 знаків включаючи пробіли
Посада (функціональне призначення)	текстове	до 64 знаків включаючи пробіли
Код ЄДРПОУ	цифрове	10 цифр
Код ДРФО	цифрове	10 цифр
Адреса	текстове	до 128 знаків включаючи пробіли
Телефон	цифрове	до 32 цифр
Адреса електронної пошти	текстове	до 128 знаків включаючи пробіли
Ім'я (DNS чи інше)	текстове	до 256 знаків включаючи пробіли
UPN-ім'я	текстове	до 256 знаків включаючи пробіли
Публікувати сертифікат назовні	логічне	Так чи ні
Ідентифікатор НБУ	цифрове	6 цифр
Код СПФМ	цифрове	6 цифр
УНЗР	цифрове	13 цифр
Код організації	текстове	до 32 знаків включаючи пробіли
Код підрозділу	текстове	до 32 знаків включаючи пробіли
Код користувача	текстове	до 32 знаків включаючи пробіли

Уточнення призначення ключів

Назва поля	Тип даних поля	Об'єм даних поля
Цифрова печатка	логічне	Так чи ні
SSL сервер	логічне	Так чи ні
SSL клієнт	логічне	Так чи ні
Автентифікація за смарт-картою	логічне	Так чи ні

Параметри сертифіката

Час введення в дію особистого ключа (сертифікат чинний з)
Час виведення з дії особистого ключа
Сертифікат чинний до

дата

: : :

: : :

: : :

час

: : :

: : :

: : :

Додаток 2
до Порядку отримання
електронних довірчих послуг у
Збройних Силах України
(пункт 4.1.)

ЖУРНАЛ ОБЛІКУ ТА ВИДАЧІ КЛЮЧОВИХ ДАНИХ
КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПISУ

(найменування установи)

Розпочато “___” _____ 20__ р.

Закінчено “___” _____ 20__ р.

На _____ аркушах

м. Київ

Продовження додатка 2

[illegible]

Згідно з оригіналом