



УКРАЇНА

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ МЕДИЧНИЙ УНІВЕРСИТЕТ

НАКАЗ

16.10.2020

Харків

№ 187-агм/н

Про організацію використання
в університеті кваліфікованих
електронних довірчих послуг

Відповідно до Закону України «Про електронні довірчі послуги», Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затвердженого постановою Кабінету Міністрів України від 19 вересня 2018 року №749, Типової інструкції з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну, затвердженої постановою КМУ від 17 січня 2018р. №55, зі змінами

НАКАЗУЮ:

1. Затвердити Порядок обліку, зберігання, застосування та знищення в Харківському національному медичному університеті кваліфікованих електронних підписів посадових осіб, кваліфікованої електронної печатки університету, кваліфікованих сертифікатів електронного підпису чи печатки та особистих ключів до них (далі - Порядок), що додається.

2. Визначити загальний відділ відповідальним підрозділом за організацію забезпечення використання в Харківському національному медичному університеті кваліфікованих електронних довірчих послуг.

3. Начальнику загального відділу Кириченко О.І. забезпечити:

3.1. підготовку та подання кваліфікованому надавачу електронних довірчих послуг інформації, необхідної для формування, скасування, блокування або поновлення кваліфікованих сертифікатів відкритих ключів посадових осіб університету;

3.2. надання допомоги посадовим особам університету під час генерації їх особистих та відкритих ключів;

3.3. ознайомлення посадових осіб університету з правилами застосування кваліфікованих електронних довірчих послуг та здійснення контролю за їх дотриманням;

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

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

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

3.7. 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;

3.8. контроль за використанням підписувачами засобів кваліфікованого електронного підпису чи печатки та зберіганням ними особистих ключів.

4. Всім співробітникам університету, які при виконанні своїх посадових обов'язків використовують засоби кваліфікованого електронного підпису чи печатки та мають чинні кваліфіковані сертифікати відкритих ключів, надати інформацію про це до загального відділу.

Термін виконання: до 29.01.2021р.

5. Проректорам, директору ННМК «Університетська клініка» ХНМУ Мальцеву А.В., директору НДІ гігієни праці та профзахворювань ХНМУ Коробчанському В.О., головному лікарю клініки НДІ ГШІЗ Мельнику О.Г., директору ННІ післядипломної освіти ХНМУ В'юну В.В., директору ННІ якості освіти ХНМУ Завгородньому І.В., директору ННІ з підготовки іноземних студентів ХНМУ Маракушину Д.І., директору Університетського стоматологічного центру ХНМУ Бірюковій М.М., директору Медичного фахового коледжу ХНМУ Лебединець Т.М., деканам факультетів, завідувачам кафедр та керівникам структурних підрозділів забезпечити виконання в підпорядкованих підрозділах вимог цього наказу.

4. Відповідальність за виконання наказу покласти на начальника загального відділу Кириченко О.І.

5. Контроль за виконанням наказу залишаю за собою.

Ректор



В.А.Капустник

ЗАТВЕРДЖЕНО

наказ ХНМУ

від 16.12.2018 № 184-оршн

ПОРЯДОК

обліку, зберігання, застосування та знищення в Харківському національному медичному університеті кваліфікованих електронних підписів посадових осіб, кваліфікованої електронної печатки університету, кваліфікованих сертифікатів електронного підпису чи печатки та особистих ключів до них

1. Цей Порядок розроблено відповідно до Законів України “Про електронні довірчі послуги” від 05.10.2017 р. №2155-VIII, “Про електронні документи та електронний документообіг” від 22.05.2003 №851-IV зі змінами, Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затверджених постановою Кабінету Міністрів України від 19.09.2018 р. № 749, і визначає умови обліку, зберігання, застосування та знищення кваліфікованого електронного підпису посадової особи, кваліфікованої електронної печатки університету, кваліфікованого сертифіката електронного підпису чи печатки та особистих ключів до них в Харківському національному медичному університеті (далі – Університет).

2. У цьому Порядку терміни вживаються у такому значенні:

засіб кваліфікованого електронного підпису чи печатки - апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки, який відповідає вимогам Закону;

захищений носій особистих ключів - засіб кваліфікованого електронного підпису чи печатки, що 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;

інформаційний обмін - відправлення, отримання та передача електронних документів, що здійснюється користувачем кваліфікованих електронних довірчих послуг в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ;

кваліфікована електронна печатка - удосконалена електронна печатка, яка створюється з використанням засобу кваліфікованої електронної печатки і базується на кваліфікованому сертифікаті електронної печатки;

кваліфіковані електронні довірчі послуги - електронні довірчі послуги, що надаються кваліфікованим надавачем електронних довірчих послуг відповідно до Закону України “Про електронні довірчі послуги (далі – Закон)”;

кваліфікований електронний підпис - удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа;

кваліфікований надавач електронних довірчих послуг - юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа - підприємець, яка надає одну або більше електронних довірчих послуг, діяльність якої відповідає вимогам цього Закону та відомості про яку внесені до Довірчого списку;

кваліфікований сертифікат відкритого ключа - сертифікат відкритого ключа, який видається кваліфікованим надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом і відповідає вимогам Закону;

компрометація особистого ключа - будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа;

користувачі електронних довірчих послуг - підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних, інші фізичні та юридичні особи, які отримують електронні довірчі послуги у надавачів таких послуг відповідно до вимог Закону;

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;

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;

3. Електронна взаємодія посадових осіб університету з іншими юридичними особами, 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, здійснюється з використанням кваліфікованих електронних довірчих послуг.

4. Університет отримує такі кваліфіковані електронні довірчі послуги:
створення, проведення перевірки та підтвердження кваліфікованого електронного підпису чи печатки;
формування, проведення перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;
формування, проведення перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту;
формування, проведення перевірки та підтвердження кваліфікованої електронної позначки часу;
здійснення реєстрованої електронної доставки;
зберігання кваліфікованих електронних підписів, печаток, позначок часу та сертифікатів, пов'язаних з цими послугами.

5. Університет для засвідчення чинності відкритого ключа використовує лише кваліфікований сертифікат відкритого ключа, а для здійснення повноважень, спрямованих на набуття, зміну чи припинення прав та/або обов'язків фізичної або юридичної особи відповідно до закону, здійснення інформаційного обміну з іншими юридичними особами, - виключно захищені носії особистих ключів.

6. Кваліфікована електронна печатка.

6.1. Для визначення достовірності походження та проведення перевірки цілісності електронних даних, а також ідентифікації університету як підписувача, у тому числі для засвідчення відповідності електронних копій електронного та паперового (фотокопія) документів оригіналу у випадках, передбачених законодавством, застосовується кваліфікована електронна печатка ХНМУ. При цьому кваліфікована електронна печатка створюється за допомогою захищених носіїв особистих ключів.

6.2. Використання електронної позначки часу під час накладання кваліфікованого електронного підпису чи печатки є обов'язковим.

6.3. Рішенням ректора університету визначається необхідність використання кваліфікованої електронної печатки та уповноважені посадові особи, відповідальні за її застосування.

7. Електронний підпис чи печатка не можуть бути визнані недійсними та позбавлені можливості розглядатися як доказ у судових справах виключно на тій підставі, що вони мають електронний вигляд або не відповідають вимогам до кваліфікованого електронного підпису чи печатки.

8. Кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису.

9. Призначення відповідальних за організацію використання в ХНМУ кваліфікованих електронних довірчих послуг.

9.1. Відповідальний за організацію використання в ХНМУ кваліфікованих електронних довірчих послуг підрозділ визначається наказом ректора університету.

9.2 Відповідальний за організацію використання в ХНМУ кваліфікованих електронних довірчих послуг підрозділ (далі – Підрозділ) забезпечує:

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

надання допомоги посадовим особам університету 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 довірчих послуг з питань використання кваліфікованих електронних довірчих послуг;

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

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

невідкладне надання кваліфікованому надавачу довірчих послуг інформації про підозру або факт компрометації особистого ключа;

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.

10. Отримання посадовими особами університету кваліфікованих електронних довірчих послуг (зокрема - кваліфікованого електронного підпису, кваліфікованої електронної печатки та особистих ключів)

10.1. Для отримання кваліфікованих електронних довірчих послуг (зокрема - кваліфікованого електронного підпису, кваліфікованої електронної печатки та особистих ключів) посадова особа університету надає до Підрозділу:

заяву на ім'я ректора з обґрунтуванням необхідності отримання зазначених послуг та візою керівника вищого рівня;

копію паспорта підписувача (1-6 сторінки), засвідчену підписувачем;

копію облікової картки платника податків підписувача, засвідчену підписувачем.

10.2. При отриманні позитивного рішення ректора Підрозділ:

готує проект наказу щодо надання права застосування кваліфікованого електронного підпису;

надає допомогу під час генерації особистих та відкритих ключів;

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

надає пакет необхідних документів кваліфікованому надавачу електронних довірчих послуг згідно зі встановленим ним регламентом надання довірчих послуг;

вносить відповідний запис до Журналу обліку, зберігання та знищення захищених носіїв особистих ключів та засобів кваліфікованого електронного підпису чи печатки (додаток 1).

10.3 Формування та видача кваліфікованого сертифіката відкритого ключа кваліфікованим надавачем електронних довірчих послуг без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті відкритого ключа, не допускаються. Ідентифікація посадової особи, яка звертається за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, здійснюється за умови її особистої присутності за паспортом громадянина України або за іншими документами, що посвідчують особу, відповідно до чинного законодавства;

10.4. У кваліфікованому сертифікаті відкритого ключа посадової особи додатково до ідентифікаційних даних фізичної особи зазначаються ідентифікаційні дані університету (найменування та код згідно з ЄДРПОУ).

10.5. Генерація пари ключів (особистого та відкритого) здійснюється посадовою особою із використанням засобів кваліфікованого електронного підпису за його особистої присутності у кваліфікованого надавача довірчих послуг або безпосередньо в університеті.

10.6. У разі звільнення або зміни посади право на застосування діючого кваліфікованого електронного підпису такою посадовою особою втрачається, а Підрозділ протягом доби звертається до кваліфікованого надавача електронних довірчих послуг з відповідною заявою про скасування кваліфікованого сертифіката відкритого ключа такої посадової особи.

11. Користувачі електронних довірчих послуг зобов'язані:

11.1. надавати повну та дійсну інформацію під час реєстрації, необхідну для його ідентифікації та формування кваліфікованих сертифікатів;

11.2. зберігати у таємниці особистий ключ та вживати всіх можливих заходів для запобігання його втрати, розкриття, зміни назви, зміни формату чи несанкціонованого використання;

11.3 не розголошувати іншим особам пароль захисту особистого ключа та ключову фразу голосової автентифікації;

11.4. не розголошувати іншим особам пароль захисту захищеного носія особистого ключа, на якому знаходиться особистий ключ;

11.5. використовувати особистий ключ виключно для мети, визначеної у кваліфікованому сертифікаті та дотримуватися інших обмежень щодо сфери використання кваліфікованого сертифіката (за наявності);

11.6. використовувати засоби кваліфікованого електронного підпису чи печатки для генерації особистих та відкритих ключів, формування та перевірки кваліфікованого електронного підпису чи печатки;

11.7. негайно інформувати Підрозділ про наступні події, що трапилися до закінчення строку чинності кваліфікованого сертифіката: компрометацію особистого ключа, компрометацію пароллю захисту особистого ключа, виявлені неточності або зміну даних, зазначених у кваліфікованому сертифікаті;

11.8. не використовувати особистий ключ у разі його компрометації;

11.9. не використовувати особистий ключ, відповідний до кваліфікованих сертифікатів, заява на скасування чи блокування яких подана до кваліфікованого надавача довірчих послуг, протягом часу з моменту подання заяви і до моменту офіційного повідомлення про скасування кваліфікованих сертифікатів;

11.10. не використовувати для накладання кваліфікованого підпису чи печатки особистий ключ, відповідний до кваліфікованого сертифіката, який скасований або блокований.

12. Скасування та блокування кваліфікованих сертифікатів відкритих ключів здійснюються у випадках, за умов та у порядку, що визначені у статті 25 Закону України “Про електронні довірчі послуги”. Кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин скасовується суб’єктом, який видав сертифікат, у разі:

12.1 подання Підрозділом заяви про скасування виданого кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача;

12.2 надходження від Підрозділу до суб’єкта, який видав сертифікат, документа, що підтверджує:

смерть фізичної особи - підписувача;

припинення діяльності створювача електронної печатки;

зміни ідентифікаційних даних користувача електронних довірчих послуг;

надання користувачем електронних довірчих послуг недостовірних ідентифікаційних даних під час формування його кваліфікованого сертифіката відкритого ключа;

факт компрометації особистого ключа користувача електронних довірчих послуг, виявлений самостійно користувачем або контролюючим органом під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг;

набрання законної сили рішенням суду про скасування кваліфікованого сертифіката відкритого ключа, оголошення підписувача померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності, визнання користувача електронних довірчих послуг банкрутом.

12.3. У разі подання повідомлення про прийняття кваліфікованим надавачем електронних довірчих послуг рішення про припинення діяльності з надання кваліфікованих електронних довірчих послуг центральний засвідчувальний орган або засвідчувальний центр на основі відповідного рішення скасовує кваліфікований сертифікат відкритого ключа, виданий цьому надавачу відповідно до вимог Закону.

12.4. Кваліфікований сертифікат відкритого ключа вважається скасованим з моменту зміни суб’єктом, який видав сертифікат, статусу кваліфікованого сертифіката відкритого ключа на скасований.

12.5. Скасований кваліфікований сертифікат відкритого ключа поновленню не підлягає.

12.6. Кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин блокується суб'єктом, який видав сертифікат, у разі:

подання користувачем електронних довірчих послуг заяви про блокування виданого йому кваліфікованого сертифіката відкритого ключа в будь-який спосіб, що забезпечує підтвердження особи-користувача;

повідомлення користувачем електронних довірчих послуг або контролюючим органом про підозру в компрометації особистого ключа користувача електронних довірчих послуг;

набрання законної сили рішенням суду про блокування кваліфікованого сертифіката відкритого ключа;

12.7. Кваліфікований сертифікат відкритого ключа, виданий центральним засвідчувальним органом, також блокується у разі прийняття рішення контролюючим органом про блокування кваліфікованих сертифікатів відкритих ключів кваліфікованого надавача електронних довірчих послуг за результатами здійснення державного нагляду (контролю) відповідно до вимог Закону.

12.8. Кваліфікований сертифікат відкритого ключа вважається заблокованим з моменту зміни суб'єктом, який видав сертифікат, статусу кваліфікованого сертифіката відкритого ключа на заблокований.

12.9. Кваліфікований сертифікат відкритого ключа, статус якого змінено на заблокований, у період блокування не використовується.

12.10. Заблокований кваліфікований сертифікат відкритого ключа не пізніше ніж протягом двох годин поновлюється суб'єктом, який видав сертифікат, у разі:

подання користувачем електронних довірчих послуг заяви про поновлення його заблокованого кваліфікованого сертифіката відкритого ключа (якщо блокування здійснено на підставі заяви про блокування кваліфікованого сертифіката відкритого ключа);

повідомлення про встановлення недостовірності інформації щодо факту компрометації особистого ключа користувачем електронних довірчих послуг або контролюючим органом, який раніше повідомив про цю підозру;

надходження до суб'єкта, який видав сертифікат, повідомлення про прийняття рішення суду про поновлення кваліфікованого сертифіката відкритого ключа, що набрало законної сили.

12.11. Заблокований кваліфікований сертифікат відкритого ключа, виданий центральним засвідчувальним органом, також поновлюється відповідно до вимог Закону в разі:

відновлення статусу кваліфікованого надавача електронних довірчих послуг;

набрання законної сили рішенням суду на користь надавача електронних довірчих послуг.

12.12. Кваліфікований сертифікат відкритого ключа, який був заблокований, відновлює свою чинність з моменту його поновлення.

12.13. Кваліфікований сертифікат відкритого ключа вважається поновленим з моменту зміни суб'єктом, який видав сертифікат, статусу кваліфікованого сертифіката відкритого ключа на поновлений.

12.14. Суб'єкт, який видав кваліфікований сертифікат відкритого ключа, повинен забезпечити доступ до інформації про дату та час зміни статусу кваліфікованого сертифіката відкритого ключа.

12.15. У разі звільнення підписувача університету або переведення до іншої державної установи, Підрозділ звертається до кваліфікованого надавача довірчих послуг для скасування його кваліфікованого сертифіката відкритого ключа із заявою, а особистий ключ не пізніше наступного дня знищується методом, що не допускає можливості його відновлення.

13. Закінчення строку чинності кваліфікованого сертифіката користувача.

13.1. Строк дії особистого та відкритого ключів дорівнює строку чинності відповідного кваліфікованого сертифіката.

13.2. Після закінчення строку чинності кваліфікованого сертифіката, він вилучається з офіційного інформаційного ресурсу кваліфікованого надавача довірчих послуг та переміщується до архіву.

13.3. Строк дії особистого ключа користувача становить не більше двох (2) років. Початком строку дії особистого ключа вважається дата та час формування кваліфікованого сертифіката, що містить відкритий ключ відповідний до особистого.

13.4. Кваліфікований надавач довірчих послуг зберігає кваліфікований сертифікат та пов'язані з ним списки відкликаних сертифікатів безстроково.

За запитом користувачів кваліфікований надавач довірчих послуг надає доступ до необхідного сертифіката та пов'язаних з ним списків відкликаних сертифікатів з його архівних записів.