

ЗАТВЕРДЖЕНО  
постановою Кабінету Міністрів  
України  
від 2018 р. №

## ПОРЯДОК

використання електронних довірчих послуг в органах  
державної влади, органах місцевого самоврядування, підприємствах,  
установах та організаціях державної форми власності

1. Цей Порядок визначає вимоги до використання, отримання та застосування електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності (далі – державні установи).

2. У цьому Порядку терміни вживаються у такому значенні:

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 нього даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання;

інформаційний обмін – відправлення, отримання та передавання електронних документів, що здійснюється користувачами (уповноваженим представником створювача) в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ.

кваліфіковані електронні довірчі послуги – електронні довірчі послуги, що надаються кваліфікованим надавачем електронних довірчих послуг відповідно до Закону України «Про електронні довірчі послуги».

контролюючий орган – спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації, що здійснює державний контроль за дотриманням вимог законодавства у сфері електронних довірчих послуг.

Інші терміни застосовуються у значенні, наведеному у Законі України «Про електронні довірчі послуги».

3. Державна установа отримує, на договірних засадах, такі кваліфіковані електронні довірчі послуги:

створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки;

формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки;

формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб-сайту;

формування, перевірки та підтвердження кваліфікованої електронної позначки часу;

реєстрованої електронної доставки;

зберігання кваліфікованих електронних підписів, печаток та сертифікатів, пов'язаних з цими послугами.

4. Порядок надання працівникам державної установи права застосування кваліфікованих електронних довірчих послуг, ведення обліку, зберігання та знищення їх особистих ключів, а також надання кваліфікованому надавачу електронних довірчих послуг інформації, необхідної для формування, скасування, блокування або поновлення кваліфікованих сертифікатів відкритих ключів користувачів державної установи, визначається рішенням її керівника, якщо інше не встановлено законодавством.

5. Використання кваліфікованих електронних довірчих послуг в державній установі забезпечує підрозділ інформаційних технологій, а у разі відсутності такого – підрозділ, що виконує відповідні функції (далі – відповідальний підрозділ), або працівник, визначений рішенням цієї установи. Зазначений підрозділ (працівник) забезпечує:

підготовку інформації, необхідної для отримання кваліфікованих електронних довірчих послуг;

надання допомоги користувачам електронних довірчих послуг під час генерації їх особистих та відкритих ключів;

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

доступ користувачів через телекомунікаційні мережі до кваліфікованого надавача електронних довірчих послуг у разі неможливості здійснення ними такого доступу із своїх робочих місць;

ведення обліку захищених носіїв особистих ключів;

ведення обліку засобів кваліфікованого електронного підпису чи печатки та носіїв, на яких зберігаються особисті ключі підписувачів чи створювачів кваліфікованих електронних печаток;

ведення обліку апаратно-програмних та апаратних носіїв особистих ключів користувача;

зберігання документів та їх електронних копій, на підставі яких отримано електронні довірчі послуги;

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

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

Подання кваліфікованому надавачу електронних довірчих послуг інформації, необхідної для отримання кваліфікованих електронних довірчих послуг, здійснюється відповідальним підрозділом (працівником) або користувачем особисто.

Генерація пари ключів (особистого та відкритого) здійснюється користувачем за особистої присутності у кваліфікованого надавача електронних довірчих послуг, що обслуговує державну установу або безпосередньо в державній установі за умови чинності раніше сформованого ним кваліфікованого сертифіката відкритого ключа.

7. Ідентифікація користувача та підтвердження цілісності даних в електронній формі здійснюються шляхом перевірки кваліфікованого електронного підпису чи печатки, з якими пов'язаний цей кваліфікований електронний підпис чи печатка.

Кваліфікований електронний підпис чи печатка вважається таким, що пройшов перевірку та отримав підтвердження, якщо:

перевірку кваліфікованого електронного підпису чи печатки проведено засобом кваліфікованого електронного підпису чи печатки;

перевіркою встановлено, що відповідно до вимог цього Закону на момент створення кваліфікованого електронного підпису чи печатки був чинним кваліфікований сертифікат електронного підпису чи печатки підписувача чи створювача електронної печатки;

за допомогою кваліфікованого сертифіката електронного підпису чи печатки здійснено ідентифікацію підписувача чи створювача електронної печатки;

під час перевірки за допомогою кваліфікованого сертифіката електронного підпису чи печатки отримано підтвердження того, що особистий ключ, який належить підписувачу чи створювачу електронної печатки, зберігається в засобі кваліфікованого електронного підпису чи печатки;

під час перевірки підтверджено цілісність електронних даних в електронній формі, з якими пов'язаний цей кваліфікований електронний підпис чи печатка.

8. Державні установи 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 відповідно до закону, застосовують виключно захищені носії особистих ключів.

9. Обмін електронними документами через систему взаємодії здійснюється виключно з дотриманням вимог до встановлених форматів даних електронного документообігу в державних установах.

Результати надання кваліфікованих електронних довірчих послуг повинні визнаватися в усіх державних установах та іншими користувачами цих послуг.

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

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

Використання кваліфікованих електронних підписів та печаток забезпечує високий рівень довіри до схем електронної ідентифікації.

11. Для визначення достовірності походження та перевірки цілісності електронних даних, а також ідентифікації державної установи як підписувача під час надання адміністративних та інших послуг в електронній формі, здійснення інформаційного обміну з іншими юридичними особами державна установа застосовує кваліфіковану електронну печатку.

У випадках передбачених законодавством для засвідчення відповідності електронних копій електронного та паперового (фотокопія) документів оригіналу державна установа застосовує кваліфіковану електронну печатку. При цьому кваліфікований електронний підпис чи печатка створюються за допомогою захищених носіїв.

Перелік електронних документів, які потребують засвідчення електронною печаткою, визначається інструкцією з діловодства державної установи на підставі актів законодавства.

Рішенням керівника державної установи визначаються порядок використання електронної печатки та уповноважені посадові особи, відповідальні за її застосування.

Державним установам надається право засвідчувати електронні копії документів, зокрема на вимогу органів судової влади та правоохоронних органів.

12. Користувач використовує у процесі виконання своїх посадових обов'язків лише особистий ключ, отриманий відповідно до пунктів 4 та 7 цього Порядку.

Після припинення виконання користувачем посадових обов'язків, для яких генерувалися особистий та відкритий ключі, користувач або державна установа звертається до кваліфікованого надавача електронних довірчих послуг для скасування його кваліфікованого сертифіката відкритого ключа, а особистий ключ знищується методом, що не допускає можливості його відновлення.

13. Відкритий ключ користувача не може мати одночасно кілька чинних кваліфікованих сертифікатів.

14. Підставами для скасування кваліфікованого сертифіката відкритого ключа користувача є надходження 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;

факт державної реєстрації припинення підприємницької діяльності фізичної особи – підприємця чи припинення діяльності в установленому законодавством порядку юридичної особи;

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;

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

15. Кваліфікований сертифікат відкритого ключа 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;

порушення користувачем електронних довірчих послуг істотних умов договору про надання кваліфікованих електронних довірчих послуг.

16. Користувачі електронних довірчих послуг зобов'язані забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа,

невідкладно повідомляти кваліфікованого надавача електронних довірчих послуг про підозру або факт компрометації особистого ключа, а також не використовувати особистий ключ у разі його компрометації та у разі скасування або блокування сертифіката відкритого ключа.

Користувач і працівник державної установи, якому надано право використання кваліфікованої електронної печатки на електронних документах, несуть відповідальність за зберігання особистих ключів, паролів та кодів доступу до них.

17. Відповідальність за організацію використання електронних довірчих послуг в державній установі несе її керівник, якщо інше не встановлено законодавством.

18. Державний контроль за дотриманням в державних установах вимог цього Порядку здійснює контролюючий орган.

**Прем'єр-міністр України**

**В. ГРОЙСМАН**