



## УЖГОРОДСЬКИЙ МІСЬКИЙ ГОЛОВА

### РОЗПОРЯДЖЕННЯ

14.06.2021

Ужгород

№ 297

#### **Про Порядок використання кваліфікованого електронного підпису та печатки в Ужгородській міській раді та її виконавчих органах**

Керуючись статтею 42 Закону України «Про місцеве самоврядування в Україні», та відповідно до Законів України «Про електронні довірчі послуги», «Про захист інформації в інформаційно-телекомунікаційних системах», постанови Кабінету Міністрів України 19.09.2018 року № 749 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності», з метою реалізації договору про надання послуги підключення інформаційної системи до Порталу Дія 01.04.2021:

1. Затвердити Порядок використання (далі - Порядок) кваліфікованого електронного підпису та печатки в міській раді та її виконавчих органах, що додається.

2. Керівникам виконавчих органів міської ради забезпечити дотримання Порядку.

3. Призначити відповідальним підрозділом за організацію використання кваліфікованих електронних довірчих послуг управління програмного та комп'ютерного забезпечення.

4. Надати дозвіл на використання електронної кваліфікованої печатки Ужгородської міської ради для здійснення інформаційного обміну з іншими юридичними особами міському голові та секретарю міської ради; на використання електронної кваліфікованої печатки виконавчого комітету Ужгородської міської ради – міському голові, заступникам міського голови, керуючому справами виконкому з урахуванням особливостей, визначених Регламентом виконавчого комітету та виконавчих органів Ужгородської міської ради.

5. Службі персоналу та спецроботи (О. Макара) вести облік посадових осіб міської ради:

- зарахованих на посаду - для надання права застосування кваліфікованого електронного підпису;

- при звільненні з посади - для скасування кваліфікованого електронного підпису та відповідних посиленних сертифікатів;

- при змінах особистих даних для скасування посиленних сертифікатів відкритих ключів та подальшої генерації особистих та відкритих ключів підписантів;

- у зв'язку з підтвердженням факту компрометації особистого ключа для скасування сертифіката.

Про надання права застосування та скасування особистих та відкритих ключів кваліфікованого електронного підпису зазначати у відповідному розпорядженні міського голови та надавати інформацію відповідальному підрозділу для вчинення відповідних дій.

6. Розпорядження міського голови 25.04.2019 № 195 визнати таким, що втратило чинність.

7. Контроль за виконанням цього розпорядження покласти на керуючого справами виконкому І. Фартушка.

**Міський голова**

**Богдан АНДРІЙВ**

ЗАТВЕРДЖЕНО  
Розпорядження міського голови  
14.06.2021 № 297

## ПОРЯДОК використання кваліфікованого електронного підпису та печатки

Порядок розроблено відповідно до законів України Законів України «Про електронні довірчі послуги», «Про захист інформації в інформаційно-телекомунікаційних системах», постанови Кабінету Міністрів України 19.09.2018 року № 749 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності» та наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3 «Про затвердження Правил посиленої сертифікації» (зі змінами та доповненнями, внесеними наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10 травня 2006 року № 50).

### I. ВИЗНАЧЕННЯ ТЕРМІНІВ

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 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;

**електронна ідентифікація** - процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи;

**електронний документ** - документ (у тому числі податкова звітність, звітність зі сплати єдиного внеску, фінансова та статистична звітність, податкові та акцизні накладні, розрахунки коригування до податкових та акцизних накладних, заяви, довідки, сервісні запити, витяги, договори, повідомлення, рішення, інші документи), які створені в електронній формі з

дотриманням вимог законодавства щодо електронного документообігу та електронних довірчих послуг;

**кваліфіковані електронні довірчі послуги** - електронні довірчі послуги, що надаються кваліфікованим надавачем електронних довірчих послуг відповідно до Закону України «Про електронні довірчі послуги»;

**електронна печатка** - електронні дані, які додаються створювачем електронної печатки до інших електронних даних або логічно з ними пов'язуються і використовуються для визначення походження та перевірки цілісності пов'язаних електронних даних;

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

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

Інші терміни вживаються у значенні, наведеному у [Законі України](#) «Про електронні довірчі послуги».

## II. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Цей Порядок поширюється на всіх працівників виконавчих органів міської ради, які при виконанні своїх службових обов'язків використовують кваліфікований електронний підпис чи печатку.

Цей Порядок поширюється на працівників виконавчих органів міської ради, які не використовують кваліфікований електронний підпис (кваліфіковану електронну печатку), але безпосередньо здійснюють організацію електронного документообігу в міській раді, а також залучаються до встановлення та налагодження програмного забезпечення.

Електронний документообіг здійснюється з використанням усіма його суб'єктами на договірних засадах послуг акредитованого центру сертифікації ключів.

**Кваліфікований електронний підпис та печатка** призначені для забезпечення діяльності міської ради, яка здійснюється з використанням електронних документів.

Кваліфікований електронний підпис використовується для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Використання кваліфікованого електронного підпису не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.

Ужгородська міська рада не застосовує кваліфікований електронний підпис:

- для складання електронних документів, які не можуть бути оригіналами у випадках, передбачених законодавством (наприклад, номерні бланки тощо);

- для складання електронних документів, які згідно із законодавством можуть бути створені лише в одному оригінальному примірнику.

Для вчинення правочинів, надання адміністративних та інших послуг в електронній формі, здійснення інформаційного обміну з іншими юридичними особами установи міська рада використовує виключно захищені носії.

### III. ОРГАНІЗАЦІЯ ТА КОНТРОЛЬ

Вимоги щодо ведення обліку, зберігання та знищення особистих ключів, а також надання кваліфікованому надавачу електронних довірчих послуг інформації, необхідної для формування, скасування, блокування або поновлення кваліфікованих сертифікатів відкритих ключів підписувачів забезпечує управління програмного та комп'ютерного забезпечення.

Про надання відповідальному підрозділу повноважень щодо застосування та контролю використання кваліфікованих електронних підписів, звернень про формування, блокування, скасування посиленних сертифікатів відкритих ключів міська рада повідомляє центр сертифікації ключів письмово чи в електронній формі або в телефонному режимі .

Відповідальний підрозділ забезпечує:

- підготовку та подавання кваліфікованому надавачу інформації, необхідної для отримання кваліфікованих електронних довірчих послуг;
- надавання 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 електронного підпису чи печатки, що використовуються в установі;
- зберігання оригіналів документів та/або їх копій (крім копій особистих документів підписувачів, що містить 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.

Контроль за використанням підписувачами засобів кваліфікованого електронного підпису здійснюють виконавчі органи міської ради або особи, відповідальні за забезпечення діловодства.

### IV. ПОРЯДОК ОРГАНІЗАЦІЇ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ З ІНШИМИ УСТАНОВАМИ ТА ОРГАНІЗАЦІЯМИ

Для здійснення електронного документообігу (інформаційного обміну) з іншими юридичними особами установи використовують виключно захищені носії.

Сторони можуть укласти між собою угоду, якою передбачатимуть здійснення спільного електронного документообігу, порядок підписання електронних документів, обміну такими документами між собою, конфіденційність та інше.

Для отримання сертифікатів відкритих ключів сторони електронного документообігу використовують відкритий каталог посилених сертифікатів на технологічному ресурсі акредитованого центру сертифікації ключів.

У разі якщо сторона електронного документообігу відмовилася від публікації своїх сертифікатів відкритих ключів, вона зобов'язана надати їх за допомогою електронної пошти або особисто через представників.

Для уникнення непорозумінь та для точного визначення моменту підписання електронного документа сторони зобов'язані при його підписанні використовувати позначку часу.

## V. УМОВИ ЗАСТОСУВАННЯ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПISУ ПІД ЧАС ВЕДЕННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Генерація особистого та відкритого ключів здійснюється підписувачем в акредитованому центрі сертифікації ключів, що обслуговує установу, або безпосередньо в установі з використанням надійних засобів кваліфікованого електронного підпису.

У посиленому сертифікаті відкритого ключа підписувача додатково зазначаються ідентифікаційні дані установи (повне найменування та код згідно з ЄДРПОУ, за якими здійснено її державну реєстрацію).

Підрозділ або відповідальна особа, яка виконує функції по застосуванню та контролю використання кваліфікованого електронного підпису, зобов'язана вести електронний архів усіх посилених сертифікатів відкритих ключів міської ради та інших установ і організацій, з якими вона веде електронний документообіг.

Підписувач використовує у процесі виконання своїх функцій лише особистий ключ, отриманий в міській раді. Використання особистого ключа у випадках, не пов'язаних з діяльністю міської ради, забороняється.

Підписувач на один і той самий момент часу може мати і використовувати лише один особистий ключ, якому відповідає відкритий ключ з чинним посиленим сертифікатом, отриманим міською радою. Це обмеження не стосується електронної печатки.

Підписувачі повинні зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері.

У разі коли згідно із законодавством необхідно засвідчити печаткою справжність підпису на документах та відповідність копій документів оригіналам, а також для забезпечення цілісності електронних даних та ідентифікації установи як підписувача під час надання адміністративних та інших послуг в електронній формі, здійснення інформаційного обміну з іншими юридичними особами установа застосовує спеціально призначений для таких цілей кваліфікований електронний підпис (кваліфікована електронна печатка).

Право проставлення електронної печатки на електронних документах надається працівникам міської ради розпорядженням міського голови.

Отримання в центрі сертифікації ключів посиленого сертифіката відкритого ключа для забезпечення застосування електронної печатки, а також генерація відповідних ключів здійснюється в тому ж порядку, що й для кваліфікованого електронного підпису.

Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з кваліфікованим електронним підписом автора.

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації, кожний з електронних примірників вважається оригіналом електронного документа.

Справжність кваліфікованого електронного підпису, накладеного на електронний документ або інші електронні дані, та цілісність цього документа (даних) перевіряється з дотриманням таких вимог:

- кваліфікований електронний підпис повинен бути підтверджений з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;

- під час перевірки повинен використовуватися посилений сертифікат ключа, чинний на момент накладення кваліфікованого електронного підпису;

- особистий ключ підписувача повинен відповідати відкритому ключу, зазначеному у сертифікаті;

- на час перевірки повинен бути чинним посилений сертифікат відкритого ключа центру сертифікації ключів та/або посилений сертифікат відкритого ключа відповідного засвідчувального центру.

Перевірка цілісності електронного документа проводиться шляхом перевірки кваліфікованого електронного підпису.

Електронний документ, що не відповідає вищезазначеним вимогам, не приймається до розгляду. Відправник такого електронного документа повідомляється про відмову в прийнятті та розгляді документа із зазначенням підстави відмови.

Датою та часом підписання електронних документів кваліфікованим електронним підписом вважається дата та час, що зазначені в позначці часу.

Підписувач зобов'язаний:

- дотримуватися вимог чинного законодавства України щодо застосування кваліфікованого електронного підпису;

- використовувати особистий ключ виключно для кваліфікованого електронного підпису, а також дотримуватися вимог щодо його використання, визначених центром сертифікації ключів;
- використовувати надійні засоби для формування та перевірки кваліфікованого електронного підпису;
- застосовувати позначку часу для підтвердження наявності електронних документів на певний момент часу;
- зберігати особистий ключ у таємниці, не допускати використання особистого ключа іншими особами;
- не використовувати особистий ключ у разі його компрометації;
- негайно інформувати центр сертифікації ключів про події, що трапилися до закінчення строку чинності сертифіката, а саме:
  - втрату або компрометацію особистого ключа;
  - втрату контролю щодо особистого ключа через компрометацію пароля, коду доступу до нього тощо;
  - виявлену неточність або зміну даних, зазначених у сертифікаті.

## VI. ПОРЯДОК ТА УМОВИ ВИКОРИСТАННЯ КВАЛІФІКОВАНОЇ ЕЛЕКТРОННОЇ ПЕЧАТКИ

Кваліфікована електронна печатка застосовується для визначення достовірності походження та проведення перевірки цілісності електронних даних, а також ідентифікації державної установи як створювача електронної печатки, у тому числі для засвідчення відповідності електронних копій електронного та паперового (фотокопія) документів оригіналу у випадках, передбачених законодавством.

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

Рішенням міського голови визначаються порядок використання кваліфікованої електронної печатки та уповноважені працівники державної установи, відповідальні за її застосування.

Кількість кваліфікованих електронних печаток, що використовуються державною установою, не обмежується.

## VII. ОБІГ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Внутрішній та зовнішній обіг електронних документів, що містять конфіденційну інформацію, здійснюється з обов'язковим використанням направленою шифрування електронних документів.

Зберігання отриманих та відправлених електронних документів, що містять конфіденційну інформацію, здійснюється відповідно до вимог чинного законодавства у цій сфері.



## VIII. ВИКОРИСТАННЯ, ЗБЕРІГАННЯ ТА ЗНИЩЕННЯ ОСОБИСТИХ КЛЮЧІВ ПІДПISУВАЧІВ

### **1. Використання особистого ключа кваліфікованого електронного підпису.**

Підписувач несе відповідальність за зберігання особистого ключа.

Використання особистого ключа підписувачем здійснюється на умовах конфіденційності. Підписувач зобов'язаний зберігати особистий ключ у таємниці та не допускати його використання іншими особами. Підписувач зобов'язаний зберігати пароль доступу до особистого ключа у таємниці.

Для забезпечення конфіденційності пароля доступу до особистого ключа підписувач має право систематично змінювати пароль, використовуючи надійні засоби кваліфікованого електронного підпису.

Копіювання особистих ключів та/або передача їх іншим особам забороняється.

У приміщенні, де знаходяться або до якого мають доступ інші особи, забороняється залишення надійних засобів кваліфікований електронний підпис з введеним особистим ключем у відсутності підписувача.

### **2. Знищення особистого ключа кваліфікованого електронного підпису.**

Після скасування сертифікатів відкритих ключів підписувачів, підрозділ або особа, яка виконує функції по застосуванню та контролю використання кваліфікованого електронного підпису, зобов'язана знищити особистий ключ методом, що не допускає можливості його відновлення.

**Про знищення особистих ключів відповідальний підрозділ виконує відповідний запис в журналі реєстрації особистих ключів із зазначенням дати, точного часу, прізвища, ім'я по батькові та посади особи, яка знищила ключ.**

## IX. БЛОКУВАННЯ, ПОНОВЛЕННЯ ТА СКАСУВАННЯ ПОСИЛЕНОГО СЕРТИФІКАТА ВІДКРИТОГО КЛЮЧА

### **1. Блокування та поновлення сертифіката відкритого ключа**

У разі компрометації або обґрунтованої підозри щодо компрометації особистого ключа, підписувач зобов'язаний терміново повідомити про це відповідальний підрозділ, який готує заяву на блокування сертифіката відкритого ключа та безпосередньо звертається до центру сертифікації ключів (регіонального пункту реєстрації заявників).

Відповідальний підрозділ здійснює фіксування кожного випадку звернення за блокуванням та поновленням сертифікатів відкритих ключів.

Блокований посилений сертифікат ключа поновлюється:

у разі подання заяви власника ключа або представника відповідального підрозділу;

за рішенням суду, що набрало законної сили;

у разі встановлення недостовірності даних про компрометацію особистого ключа.

## **2. Скасування сертифіката відкритого ключа**

Сертифікат відкритого ключа підписувача скасовується у разі:

- припинення діяльності юридичної особи – власника ключа;
- смерті фізичної особи – підписувача або оголошення його померлим за рішенням суду;
- визнання підписувача недієздатним за рішенням суду;
- надання недостовірних даних про підписувача;
- закінчення строку чинності сертифіката ключа;
- подання заяви власника ключа або його уповноваженого представника;
- зміни даних про підписувача, що зазначені у сертифікаті відкритого ключа;
- звільнення підписувача;
- компрометації особистого ключа.

Відповідальний підрозділ спільно з службою персоналу та спецроботи:

- у разі припинення діяльності виконавчих органів міської ради повідомляє центр сертифікації ключів про необхідність скасування сертифікатів відкритих ключів із зазначенням дати такого скасування;

- у разі смерті фізичної особи – підписувача, оголошення його померлим за рішенням суду, визнання підписувача недієздатним за рішенням суду з моменту підтвердження даних про смерть фізичної особи – підписувача або з набранням відповідними рішеннями суду законної сили повідомляє центр сертифікації ключів та надає заяву про скасування сертифіката відкритого ключа;

- у разі надання недостовірних даних про підписувача, зміни даних про підписувача, що зазначені у сертифікаті відкритого ключа, невідкладно, з моменту встановлення подання недостовірних даних або зміни даних про підписувача, надає центру сертифікації ключів заяву на скасування сертифіката відкритого ключа та у разі необхідності формування нового сертифіката відкритого ключа – заяву на формування сертифіката з новими даними про підписувача;

- після звільнення підписувача звертається до центру сертифікації ключів для скасування посиленого сертифіката його відкритого ключа;

- у разі компрометації особистого ключа підписувача терміново повідомляє центр сертифікації ключів та надає заяву на скасування сертифіката відкритого ключа.

---