



КАБІНЕТ МІНІСТРІВ УКРАЇНИ

**ПОСТАНОВА**  
**від 28 жовтня 2004 р. N 1452**  
**Київ**

Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності

*{ Із змінами, внесеними згідно з Постановою КМ  
N 1700 ( 1700-2006-п ) від 08.12.2006 }*

Відповідно до статті 5 Закону України "Про електронний цифровий підпис" ( [852-15](#) ) Кабінет Міністрів України **п о с т а н о в л я є**:

1. Затвердити Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності (додається).

2. Міністерству транспорту та зв'язку за погодженням з Міністерством економіки та з питань європейської інтеграції затвердити в шестимісячний строк граничні ціни (тарифи) на послуги, пов'язані з електронним цифровим підписом, що надаються органам державної влади, органам місцевого самоврядування, підприємствам, установам та організаціям державної форми власності акредитованими центрами сертифікації ключів.

Прем'єр-міністр України

В.ЯНУКОВИЧ

Інд. 49

ЗАТВЕРДЖЕНО  
постановою Кабінету Міністрів України  
від 28 жовтня 2004 р. N 1452

**ПОРЯДОК**  
**застосування електронного цифрового підпису органами**  
**державної влади, органами місцевого самоврядування,**  
**підприємствами, установами та організаціями**  
**державної форми власності**

1. Цей Порядок визначає вимоги до застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності (далі - установи).

2. Установа застосовує електронний цифровий підпис лише за умови використання надійних засобів електронного цифрового підпису, що повинне бути підтверджено сертифікатом відповідності або позитивним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, отриманим на ці засоби від Адміністрації Держспецзв'язку, та наявності посиленних сертифікатів відкритих ключів у своїх працівників - підписувачів.

{ Пункт 2 із змінами, внесеними згідно з Постановою КМ N 1700 ( [1700-2006-п](#) ) від [08.12.2006](#) }

3. Установа застосовує електронний цифровий підпис для вчинення правочинів за участю інших юридичних та фізичних осіб лише за наявності у них посиленних сертифікатів відкритих ключів.

4. Установа не застосовує електронний цифровий підпис:

для складання електронних документів, які не можуть бути оригіналами у випадках, передбачених законодавством;

для вчинення правочинів на суму, що перевищує 1 млн. гривень.

5. Установа отримує на договірних засадах послуги, пов'язані з електронним цифровим підписом, від акредитованого центру сертифікації ключів. При цьому установа може отримувати такі послуги лише від одного акредитованого центру сертифікації ключів. Використання підписувачами особистих ключів, відповідні відкриті ключі яких засвідчені іншими акредитованими центрами сертифікації ключів, забороняється.

6. Граничні ціни (тарифи) на послуги, пов'язані з електронним цифровим підписом, що надаються установам акредитованими центрами сертифікації ключів, установлюються Мінтранспозв'язку за погодженням з Мінекономіки.

7. Установа здійснює обмін інформацією з акредитованим центром сертифікації ключів через телекомунікаційні мережі.

8. Відповідальність за організацію застосування електронного цифрового підпису в установі несе її керівник, якщо інше не встановлено законодавством.

9. Застосування електронного цифрового підпису в установі забезпечує підрозділ інформаційних технологій, а у разі відсутності такого - підрозділ, що виконує відповідні функції

(далі - відповідальний підрозділ), або працівник, спеціально визначений наказом керівника цієї установи. Зазначений підрозділ (працівник) забезпечує:

підготовку та надання акредитованому центру сертифікації ключів інформації, необхідної для формування посилених сертифікатів відкритих ключів підписувачів;

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

подання до акредитованого центру сертифікації ключів звернень про скасування, блокування або поновлення посилених сертифікатів відкритих ключів підписувачів;

доступ підписувачів через телекомунікаційні мережі до акредитованих центрів сертифікації ключів у разі неможливості здійснення ними такого доступу із своїх робочих місць;

ведення обліку засобів електронного цифрового підпису, що використовуються в установі;

ведення обліку носіїв особистих ключів підписувачів;

зберігання документів, на підставі яких було сформовано посилені сертифікати відкритих ключів підписувачів;

контроль за використанням підписувачами засобів електронного цифрового підпису та зберіганням ними особистих ключів.

10. Порядок надання працівникам установи права застосування електронного цифрового підпису, ведення обліку, зберігання та знищення їх особистих ключів, а також надання акредитованому центру сертифікації ключів інформації, необхідної для формування, скасування, блокування або поновлення посилених сертифікатів відкритих ключів підписувачів установи, визначається наказом її керівника, якщо інше не встановлено законодавством.

11. Генерація особистого та відкритого ключів здійснюється підписувачем безпосередньо в установі або в акредитованому центрі сертифікації ключів, що її обслуговує. У разі потреби під час генерації ключів підписувачеві надається допомога персоналом відповідального підрозділу (спеціально визначеним працівником) або персоналом акредитованого центру сертифікації ключів.

12. У посиленому сертифікаті відкритого ключа підписувача додатково зазначається його належність до установи та посада, яку він займає.

13. У разі коли згідно із законодавством необхідне засвідчення печаткою справжності підпису на документах та відповідності копій документів оригіналам, установа застосовує спеціально призначений для таких цілей електронний цифровий підпис (далі - електронна печатка).

Установа застосовує електронну печатку лише за наявності у неї відповідної печатки, що застосовується для документів на папері.

У посиленому сертифікаті відкритого ключа, що використовується установою для електронної печатки, додатково зазначається спеціальне призначення електронного цифрового підпису та сфера його застосування, а також відтворюється текстова інформація, розміщена на відповідній печатці.

14. Право проставлення електронної печатки на електронних документах надається лише тому працівнику установи, який проставляє відповідну печатку на документах на папері.

Отримання в акредитованому 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 електронного цифрового підпису.

15. Підписувач може застосовувати електронний цифровий підпис лише після отримання установою від акредитованого центру сертифікації ключів посиленого сертифіката його відкритого ключа.

Після звільнення підписувача установа звертається до акредитованого центру сертифікації ключів для скасування посиленого сертифіката його відкритого ключа, а особистий ключ знищується методом, що не допускає можливості його відновлення.

16. Підписувач використовує у процесі виконання своїх функцій лише особистий ключ, отриманий в установі. Використання особистого ключа у випадках, не пов'язаних з діяльністю установи, забороняється.

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

18. Підписувач несе відповідальність за зберігання особистого ключа.

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

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

електронний цифровий 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 електронного цифрового підпису;

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

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

21. Контроль за виконанням в установах вимог цього Порядку здійснює Адміністрація Держспецзв'язку.

*{ Пункт 21 із змінами, внесеними згідно з Постановою КМ N 1700 ( 1700-2006-п ) від 08.12.2006 }*