



КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА
від 13 липня 2004 р. N 903
Київ

Про затвердження Порядку акредитації
центру сертифікації ключів

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

Відповідно до статті 9 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 акредитації центру сертифікації ключів, що додається.
2. Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки розробити та затвердити у шестимісячний строк вимоги до обслуговування та використання посилених сертифікатів відкритих ключів.

Прем'єр-міністр України

В.ЯНУКОВИЧ

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 13 липня 2004 р. N 903

ПОРЯДОК
акредитації центру сертифікації ключів

1. Цей Порядок визначає процедуру акредитації центру сертифікації ключів (далі - центр), умови надання центром послуг електронного цифрового підпису, вимоги до його персоналу та захисту інформації.

2. Терміни, які вживаються у цьому Порядку, мають таке значення:

контролюючий орган - Адміністрація Держспецзв'язку; { Абзац другий пункту 2 із змінами, внесеними згідно з Постановою КМ N 1700 (1700-2006-п) від 08.12.2006 }

програмно-технічний комплекс - апаратні, апаратно-програмні та програмні засоби акредитованого центру, що забезпечують виконання функцій, пов'язаних з наданням послуг електронного цифрового підпису;

спеціальне приміщення - приміщення, яке відповідає вимогам технічного захисту інформації;

правила посиленої сертифікації - затверджені в установленому порядку вимоги до обслуговування та використання посилених сертифікатів відкритих ключів (далі - сертифікати);

регламент роботи акредитованого центру - нормативний документ, що визначає організаційні, технічні та інші умови діяльності акредитованого центру під час надання послуг електронного цифрового підпису;

список відкликаних сертифікатів - перелік блокованих та скасованих сертифікатів, що формується та розповсюджується акредитованим центром;

статус сертифіката - стан посиленого сертифіката ключа (чинний, блокований, скасований) на конкретний момент.

Інші терміни застосовуються у значенні, наведеному у Законах України "Про електронний цифровий підпис" ([852-15](#)), "Про телекомунікації" ([1280-15](#)), інших нормативно-правових актах з питань інформатизації та захисту інформації.

3. Акредитація центру здійснюється на добровільних засадах.

4. Інформація про акредитацію центру сертифікації ключів та припинення його діяльності оприлюднюється центральним засвідчувальним органом на власному веб-сайті та у друкованих засобах масової інформації.

5. До проведення акредитації центр вносить на спеціальний рахунок, відкритий у банківській установі, кошти у розмірі стократною мінімальної заробітної плати для забезпечення відшкодування збитків, які можуть бути завдані підписувачам, користувачам або третім особам внаслідок неналежного виконання акредитованим центром своїх зобов'язань.

Наявність спеціального рахунка не обов'язкова для акредитованого центру, який надає пов'язані з електронним цифровим підписом послуги виключно органам державної влади.

6. Для проведення акредитації центр, що засвідчив свій відкритий ключ у центральному засвідчувальному органі та вніс кошти на спеціальний рахунок, подає до нього заяву разом із документами, перелік яких наведено у додатку 1.

У заяві зазначаються:

повне найменування юридичної особи, посада, прізвище, ім'я та по батькові її керівника (прізвище, ім'я та по батькові фізичної особи - суб'єкта підприємницької діяльності, серія і номер паспорта, ким і коли виданий);

організаційно-правова форма;

код згідно з ЄДРПОУ (ідентифікаційний номер фізичної особи - платника податків та інших обов'язкових платежів);

номер поточного рахунка та найменування банківської установи;

місцезнаходження (місце проживання);

номери телефонів;

електронна адреса електронного інформаційного ресурсу;

відомості про реєстрацію відкритого ключа в центральному засвідчувальному органі.

7. На підставі заяви та доданих до неї документів центральний засвідчувальний орган у строк не більше ніж 45 днів від дати подання заяви приймає рішення про акредитацію центру або про відмову в акредитації.

У разі необхідності центральний засвідчувальний орган здійснює перевірку центру на відповідність вимогам цього Порядку.

8. Центр вважається акредитованим від дня внесення до Реєстру суб'єктів, які надають послуги, пов'язані з електронним цифровим підписом (далі - Реєстр), що ведеться центральним засвідчувальним органом, основних даних (реквізитів) акредитованого центру, зазначених у пункті 5 цього Порядку, відомостей про дату прийняття та номер рішення про акредитацію, серію та номер свідоцтва, а також строк дії свідоцтва.

9. У разі прийняття центральним засвідчувальним органом рішення про акредитацію, центрові видається свідоцтво про акредитацію (далі - свідоцтво) за зразком, наведеним у додатку 2.

Копії рішення про акредитацію та свідоцтва надсилаються до контролюючого органу.

10. Свідоцтво видається уповноваженому представнику центру протягом п'яти робочих днів від дати внесення відповідного запису до Реєстру.

11. У разі зміни відомостей, які внесені до Реєстру, акредитований центр у триденний строк повідомляє про це центральний засвідчувальний орган.

12. У разі пошкодження або втрати свідоцтва центрові видається протягом десяти днів від дати подання відповідної заяви його дублікат.

Відомості про видачу дубліката вносяться до Реєстру.

13. Акредитований центр проходить повторну акредитацію у разі:

зміни основних даних (реквізитів), які зазначаються у свідоцтві;

закінчення строку дії свідоцтва;

закінчення строку дії атестата відповідності комплексної системи захисту інформації або внесення до програмно-технічного комплексу акредитованого центру змін, які потребують модернізації комплексної системи захисту інформації;

закінчення строку дії сертифіката відповідності або позитивного експертного висновку за результатами державної експертизи у сфері криптографічного захисту інформації;

повідомлення контролюючим органом щодо порушення порядку проведення акредитації.

Повторна акредитація здійснюється згідно з пунктами 5-10 цього Порядку.

14. Рішення про скасування акредитації центральний засвідчувальний орган приймає у разі:

повідомлення контролюючим органом про порушення акредитованим центром законодавства;

неукладення протягом року жодного договору про надання послуг цифрового підпису;

неповнення спеціального рахунка для забезпечення відшкодування збитків;

невиконання акредитованим центром встановлених вимог;

прийняття акредитованим центром рішення про припинення діяльності.

15. У разі прийняття рішення про скасування акредитації свідоцтво анулюється.

16. Відомості про скасування акредитації та анулювання свідоцтва центральний засвідчувальний орган вносить до Реєстру і повідомляє про це акредитований центр та контролюючий орган із зазначенням підстав скасування акредитації.

17. Центр, якому було відмовлено в акредитації у зв'язку з поданням недостовірної інформації або акредитацію якого було скасовано, не може бути акредитований протягом року від дати прийняття рішення про відмову в акредитації або про скасування акредитації.

18. Рішення про відмову в акредитації або скасування акредитації може бути оскаржено в судовому порядку.

19. За проведення акредитації справляється плата у розмірі, встановленому центральним засвідчувальним органом за погодженням з Мінекономіки.

20. Акредитований центр:

забезпечує виконання вимог щодо надання послуг електронного цифрового підпису згідно із законом;

інформує підписувача про обмеження використання електронного цифрового підпису та порядок відшкодування збитків;

виконує приписи контролюючого органу;

надає допомогу підписувачам під час генерації особистих та відкритих ключів у разі отримання від них відповідного звернення та вживає заходів щодо забезпечення безпеки інформації під час генерації;

забезпечує розташування засобів програмно-технічного комплексу, за допомогою яких здійснюється надання послуг сертифікації та відкриття, в спеціальних приміщеннях та їх охорону;

забезпечує збереження програмно-технічного комплексу, іншого майна та запобігання безконтрольному проникненню в приміщення акредитованого центру сторонніх осіб;

використовує програмно-технічний комплекс, засоби криптографічного захисту інформації, в тому числі засоби електронного цифрового підпису, та формати даних, які ними використовуються, відповідно до вимог спеціально уповноваженого органу у сфері криптографічного та технічного захисту інформації.

21. Надання послуг електронного цифрового підпису здійснюється акредитованим центром згідно з правилами посиленої сертифікації та регламентом роботи цього центру.

22. Акредитований центр під час надання послуг електронного цифрового підпису фізичним та юридичним особам, фізичним особам-підприємцям зобов'язаний дотримуватися таких вимог:

встановлювати відповідно до законодавства фізичну особу, фізичну особу-підприємця, юридичну особу та уповноваженого представника юридичної особи, які звернулися до акредитованого центру з метою формування сертифіката;

перевіряти дані, обов'язкові для формування сертифіката, і дані, які вносяться до нього на вимогу підписувача;

реєструвати та вести облік звернень фізичних та юридичних осіб, на підставі яких були сформовані сертифікати;

встановлювати належність підписувачу особистого ключа та його відповідність відкритому ключу, якщо їх генерація здійснювалася не в акредитованому центрі.

23. У разі використання коштів із спеціального рахунка для відшкодування завданих збитків акредитований центр зобов'язаний протягом 30 днів від дати здійснення такого відшкодування поповнити спеціальний рахунок до встановленого розміру.

24. Керівник та інші посадові особи акредитованого центру, які безпосередньо беруть участь в обслуговуванні посилених сертифікатів ключів (далі - посадові особи), повинні мати відповідний досвід роботи не менше ніж три роки.

25. Обов'язковими в акредитованому центрі є посади адміністратора реєстрації, адміністратора сертифікації, адміністратора безпеки та системного адміністратора.

Адміністратор реєстрації відповідає за встановлення фізичних та юридичних осіб, фізичних осіб-підприємців під час формування, блокування, поновлення та скасування сертифіката.

Адміністратор сертифікації відповідає за формування сертифікатів, списків відкликаних сертифікатів, збереження та використання особистого ключа акредитованого центру.

Адміністратор безпеки відповідає за належне функціонування комплексної системи захисту інформації та входить до складу служби захисту інформації акредитованого центру. Забороняється суміщення посади адміністратора безпеки з іншими посадами.

Системний адміністратор відповідає за функціонування програмно-технічного комплексу.

26. Керівник та посадові особи акредитованого центру несуть відповідальність за розголошення конфіденційної інформації, зокрема відомостей про персональні дані, згідно із законом.

27. Акредитований центр під час надання послуги сертифікації фізичним та юридичним особам зобов'язаний:

генерувати відкритий та особистий ключі підписувача;

формувати сертифікат згідно із законом.

Під час формування сертифіката акредитований центр:

присвоює унікальний реєстраційний номер сертифікату;

перевіряє унікальність відкритого ключа підписувача в реєстрі чинних, блокованих та скасованих сертифікатів;

включає дані про обмеження використання електронного цифрового підпису;

включає електронну адресу електронного інформаційного ресурсу, де публікується список відкликаних сертифікатів акредитованого центру;

на вимогу підписувача включає додаткові дані.

Сертифікат підписувача, сформований акредитованим центром, чинний не більше ніж два роки.

Сертифікат акредитованого центру чинний не більше ніж п'ять років.

28. Особистий ключ акредитованого центру використовується виключно для формування сертифікатів підписувачів, даних про статус сертифіката та надання послуги фіксування часу.

Після закінчення терміну чинності особистий ключ та всі його резервні копії знищуються методом, що не допускає можливості їх відновлення.

29. Резервні копії сертифікатів та списку відкликаних сертифікатів, сформованих в акредитованому центрі, зберігаються в приміщенні, територіально відокремленому від приміщення акредитованого центру, із забезпеченням захисту від несанкціонованого доступу.

30. Акредитований центр зобов'язаний забезпечити можливість цілодобового вільного доступу користувачів з використанням телекомунікаційних мереж загального користування до:

сертифікатів підписувачів за їх згодою;

даних про статус сертифікатів ключів;

сертифіката акредитованого центру;

нормативних документів з питань надання послуг електронного цифрового підпису, зокрема до правил посиленої сертифікації та регламенту роботи акредитованого центру, а також порядку здійснення перевірки чинності сертифіката.

Надання користувачам достовірних даних про статус сертифікатів здійснюється за їх запитом у реальному часі та/або з використанням списку відкликаних сертифікатів відповідно до регламенту роботи акредитованого центру.

31. Акредитований центр зобов'язаний забезпечити:

цілодобовий прийом звернень про скасування та блокування сертифікатів;

прийом звернень про поновлення сертифікатів;

перевірку законності звернень про блокування, поновлення та скасування сертифікатів.

Час між отриманням звернення підписувача або його уповноваженого представника про скасування, блокування сертифіката та внесенням змін до списку відкликаних сертифікатів, доступних користувачам, не повинен перевищувати двох годин.

Час формування, скасування, блокування та поновлення сертифікатів встановлюється за київським часом і синхронізується з Всесвітнім координованим часом (UTC) з точністю до однієї секунди.

Формування, скасування, блокування та поновлення сертифікатів здійснюється за участю або під контролем не менше ніж двох посадових осіб акредитованого центру відповідно до їх посадових обов'язків.

32. У договорі між акредитованим центром та підписувачем щодо надання послуг електронного цифрового підпису додатково зазначається про згоду або незгоду підписувача надавати вільний доступ до його сертифіката користувачам та порядок взаємодії між підписувачем і акредитованим центром.

33. Акредитований центр може надавати інші послуги, які не суперечать вимогам законодавства та цього Порядку.

34. Захист інформації, яка обробляється в акредитованому центрі, забезпечується в результаті здійснення комплексу технічних, криптографічних, організаційних та інших заходів і впровадження комплексної системи захисту інформації.

35. Комплексна система захисту інформації повинна мати атестат відповідності вимогам захисту інформації.

36. В акредитованому центрі створюється служба захисту інформації, яка забезпечує вирішення питань, пов'язаних із проектуванням, розробленням і модернізацією, введенням в експлуатацію, обслуговуванням і підтримкою працездатності комплексної системи захисту інформації, а також контролем за станом захищеності інформації.

ПЕРЕЛІК
документів, що подаються разом із
заявою про акредитацію

1. Копії установчих документів, засвідчені в установленому порядку (для юридичної особи).
2. Копія свідоцтва про державну реєстрацію суб'єкта підприємницької діяльності, засвідчена в установленому порядку.
3. Копія довідки про внесення юридичної особи до ЄДРПОУ, засвідчена в установленому порядку.
4. Копії паспорта або іншого документа, що підтверджують повноваження фізичної особи на представлення інтересів суб'єкта підприємницької діяльності.
5. Копія документа, що підтверджує право власності центру сертифікації ключів на окреме приміщення або оренду такого приміщення, засвідчена в установленому порядку.
6. Копія документа про внесення на спеціальний рахунок коштів для забезпечення відшкодування збитків, які можуть бути завдані акредитованим центром підписувачам, користувачам або третім особам внаслідок неналежного виконання своїх зобов'язань.
7. Документ, що підтверджує внесення плати за проведення акредитації.
8. Копія атестата відповідності комплексної системи захисту інформації вимогам нормативних документів у сфері захисту інформації.
9. Копії сертифікатів відповідності або позитивних експертних висновків за результатами державної експертизи у сфері криптографічного захисту інформації.
10. Список посадових осіб центру сертифікації ключів та засвідчені в установленому порядку копії документів про рівень освіти і кваліфікації керівника центру сертифікації ключів та посадових осіб, обов'язки яких безпосередньо пов'язані з наданням послуг електронного цифрового підпису та обслуговуванням посилених сертифікатів відкритих ключів.
11. Регламент роботи центру сертифікації ключів, затверджений керівником та погоджений контролюючим органом.
12. Положення, яким визначаються посадові обов'язки, кваліфікаційні вимоги та відповідальність посадових осіб центру сертифікації ключів.
13. Положення про службу захисту інформації центру сертифікації ключів, затверджене його керівником.

14. План-схема приміщень центру сертифікації ключів та порядок доступу до спеціальних приміщень.

15. Порядок зберігання окремих резервних копій посилених сертифікатів ключів та списків відкликаних сертифікатів, сформованих акредитованим центром.

16. Порядок синхронізації з Всесвітнім координованим часом (UTC).

17. Відомості про ліцензії на право провадження господарської діяльності в галузі криптографічного або технічного захисту інформації (у разі наявності).

Зразок

Центральний засвідчувальний орган

СВІДОЦТВО
про акредитацію центру сертифікації ключів

Серія _____

N _____

Згідно з рішенням центрального засвідчувального органу від _____ 200__ р.
N _____

_____ (повне найменування юридичної особи (прізвище,

ім'я та по батькові фізичної особи)),

_____ код згідно з ЄДРПОУ (ідентифікаційний номер фізичної

_____ особи - платника податків та інших обов'язкових платежів)

відповідає вимогам до акредитованого центру сертифікації ключів та внесен _____
_____ 200__ р. в Реєстр суб'єктів, які надають послуги
електронного цифрового підпису, за N _____

Місцезнаходження акредитованого центру сертифікації ключів _____

Свідоцтво дійсне до _____ 20__ р.

_____ (посада керівника органу)

_____ (підпис)

_____ (ініціали та прізвище)

М.П.