|  |  |
| --- | --- |
|  | ЗАТВЕРДЖЕНО Постанова Кабінету Міністрів України від \_\_\_\_\_\_\_\_\_\_\_ 2016 року № \_\_\_\_ |

**ПОРЯДОК**
**внесення засобів електронного цифрового підпису та засобів криптографічного захисту інформації до безконтактного електронного носія, що міститься у паспорті громадянина України, та надання послуг електронного цифрового підпису з використанням паспорта громадянина України з імплантованим безконтактним електронним носієм**

1. Цей Порядок установлює з урахуванням вимог Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», «Про електронний цифровий підпис», законодавства у сфері надання послуг електронного цифрового підпису (далі - ЕЦП) та криптографічного захисту інформації (далі – шифрування), міжнародних стандартів та рекомендацій Міжнародної організації цивільної авіації (ІКАО), механізм здійснення операцій із внесення надійних засобів ЕЦП та засобів шифрування до безконтактного електронного носія (далі – БЕН), який імплантовано до паспорта громадянина України, їх використання та надання послуг ЕЦП з використанням паспорта громадянина України у формі картки.
2. У цьому Порядку терміни вживаються в таких значеннях:

авторизація – процедура отримання дозволу на проведення операцій внесення до БЕН додаткової змінної інформації, визначеної у Законі України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», інформації до захищених груп даних та зчитування інформації, внесеної до БЕН;

безконтактний електронний носій (БЕН) – електронний носій, який імплантований у паспорт громадянина України, є захищеним носієм ключових даних та надійним засобом ЕЦП і шифрування та використовується з метою здійснення комплексу заходів, пов’язаних з ідентифікацією особи та накладанням ЕЦП;

групи даних – області постійного запам’ятовуючого пристрою БЕН, до яких вноситься інформація, визначена в Законі України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»;

захищені групи даних – області постійного запам’ятовуючого пристрою БЕН, до яких вноситься набір електронних даних, за допомогою яких забезпечується можливість підтвердження цілісності даних БЕН, генерації ключових даних та накладання ЕЦП;

підписувач - фізична особа - власник паспорта громадянина України з імплантованим БЕН, яка на законних підставах володіє особистим ключем та від свого імені накладає електронний цифровий підпис під час створення електронного документа;

ПАК1 – персональний авторизаційний код, який складається з 8 цифр, відомий лише особі, на ім’я якої оформлено паспорт, і призначений для розблокування ПІН1;

ПАК2 – персональний авторизаційний код, який складається з 8 цифр, відомий лише особі, на ім’я якої оформлено паспорт, і призначений для розблокування ПІН2;

ПІН1– персональний ідентифікаційний номер, який складається з 4 цифр, відомий лише особі, на ім’я якої оформлено паспорт, і призначений для ідентифікації та авторизації доступу до БЕН під час здійснення операцій внесення додаткової змінної інформації до БЕН;

ПІН2 – персональний ідентифікаційний номер, який складається з 4 цифр, відомий лише особі, на ім’я якої оформлено паспорт, і призначений для здійснення операцій зчитування із захищених груп даних БЕН.

Інші терміни використовуються у значенні, наведеному в Законі України «Про електронний цифровий підпис».

1. Послуги ЕЦП у частині, що стосується обслуговування посилених сертифікатів відкритих ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення) фізичних осіб - власників паспорта громадянина України з імплантованим БЕН, надання інформації щодо чинних, скасованих і блокованих посилених сертифікатів відкритих ключів (далі – сертифікатів ключів), послуги фіксування часу, консультації та інші послуги, визначені Законом України «Про електронний цифровий підпис», надаються Акредитованим центром сертифікації ключів Міністерства внутрішніх справ України (далі – Центр).
2. Уповноважені суб’єкти, визначені у Законі України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» як такі, що мають право видачі паспорта громадянина України, здійснюють представництво Центру в порядку, передбаченому Цивільним кодексом України, організаційно-розпорядчими актами Міністерства внутрішніх справ України та Регламентом роботи Центру.
3. На суб’єктів, що здійснюють представництво Центру, покладається відповідальність за невиконання чи неналежне виконання своїх обов’язків згідно з чинним законодавством у сфері надання послуг ЕЦП.
4. Регламент роботи Центру розроблюється та узгоджується у відповідності до вимог законодавства у сфері надання послуг ЕЦП.
5. Суб’єкти, що здійснюють представництво Центру, уповноважені здійснювати надання таких послуг ЕЦП та виконання таких процедур:

- приймання від громадян, що отримують паспорт громадянина України з імплантованим БЕН, заяв про реєстрацію та укладання договорів про надання послуг ЕЦП;

- встановлення (ідентифікація) особи;

- надання у користування надійних засобів ЕЦП та засобів шифрування, внесених до паспортів громадянина України з імплантованим БЕН;

- допомога під час генерації ключів.

1. Особливості надання послуг ЕЦП фізичним особам – власникам паспорта громадянина України з імплантованим БЕН визначаються Регламентом роботи Центру.

Особливості надання послуг ЕЦП особам з обмеженими можливостями та забезпечення їх надійними засобами ЕЦП та засобами шифрування, внесених до паспортів громадянина України з імплантованим БЕН, визначаються Регламентом роботи Центру та наказами Міністерства внутрішніх справ України.

1. Внесення надійних засобів ЕЦП та шифрування до паспортів громадянина України з імплантованим БЕН здійснюється на етапі виготовлення бланків документів з урахуванням вимог Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус».
2. Надійні засоби ЕЦП та засоби шифрування, які вносяться до паспортів громадянина України з імплантованим БЕН, повинні забезпечувати:

- генерацію та зберігання в захищеній енергонезалежній області пам’яті БЕН пар ключів (особистий та відкритий ключі), які використовуються для накладення та перевірки ЕЦП, та пар ключів, які використовуються для протоколу узгодження ключів шифрування;

- можливість зберігання в захищеній енергонезалежній області пам’яті БЕН не менше п’яти пар ключів (особистий та відкритий ключі), які використовуються для накладення та перевірки ЕЦП, та п’яти пар ключів, які використовуються для протоколу узгодження ключів шифрування;

- захист від несанкціонованого доступу до функцій криптографічних перетворень (виклик таких функцій здійснюється після введення ПІН2);

- неможливість безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.

1. Центр повинен забезпечувати відповідність сертифікатів ключів вимогам законодавства до їх форматів та щодо строків їх чинності.
2. Генерація першої пари ключів, які використовуються для накладення та перевірки ЕЦП, та першої пари ключів, які використовуються для протоколу узгодження ключів шифрування, здійснюється фізичною особою - власником паспорта громадянина України з імплантованим БЕН в уповноваженого суб’єкта, що здійснює представництво Центру, за допомогою програмних засобів робочої станції для оформлення та видачі документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус, з комплектом обладнання для зняття біомертичних даних (параметрів) і реєстрації/зняття з реєстрації місць проживання/перебування громадян України, іноземців та осіб без громадянства Державної міграційної служби України (далі – РС ДМС).
3. Програмні засоби РС ДМС повинні забезпечувати виклик функцій криптографічних перетворень, направлених на генерацію ключових пар в надійних засобах ЕЦП, внесених до паспортів громадянина України з імплантованим БЕН, лише після зміни початкових значень ПІН1(2) та ПАК1(2).
4. Зміна початкових значень ПІН1(2) та ПАК1(2) повинна здійснюватись виключно фізичною особою - власником паспорта громадянина України з імплантованим БЕН після її встановлення (ідентифікації) працівником суб’єкта, що здійснює представництво Центру.
5. Після генерації пар ключів, програмними засобами РС ДМС формуються та автоматично відправляються до Центру обробки даних Єдиного державного демографічного реєстру запити на реєстрацію фізичної особи - власника паспорта громадянина України з імплантованим БЕН в якості підписувача та запити на формування сертифікатів ключів ЕЦП та шифрування.
6. Запит на реєстрацію особи в якості підписувача містить дані про фізичну особу - власника паспорта громадянина України з імплантованим БЕН, які необхідні для подальшого формування Центром сертифікатів ключів.
7. Запит на формування сертифікатів ключів ЕЦП та шифрування містить відповідні відкриті ключі, що отримані під час генерації пар ключів, та формується у відповідності до міжнародних рекомендацій у сфері забезпечення інтероперабельності системи ЕЦП RFC 2986 «PKCS #10: Certification Request Syntax Specification».
8. Програмними засобами Центру обробки даних Єдиного державного демографічного реєстру через програмні засоби віддалених автоматизованих робочих місць забезпечується доступ уповноважених представників суб’єкта, що здійснює представництво Центру, до процесів обробки запитів на реєстрацію особи в якості підписувача та запитів на формування сертифікатів ключів ЕЦП та шифрування. Результатом процесів обробки є передача загаданих вище запитів до Центру для формування відповідних сертифікатів.
9. Всі події, пов’язані із формуванням та відправкою запитів на реєстрацію фізичної особи - власника паспорта громадянина України з імплантованим БЕН в якості підписувача та запитів на формування сертифікатів ключів ЕЦП та шифрування, повинні вноситись до журналу реєстрації подій Єдиної інформаційно-аналітичної системи управління міграційними процесами Державної міграційної служби України (далі – відомча інформаційна система, ВІС) із забезпеченням ідентифікації ініціатора події - працівника суб’єкта, що здійснює представництво Центру, за допомогою сертифіката ключа, власником якого є вказаний працівник.
10. Про отримання запиту на реєстрацію фізичної особи - власника паспорта громадянина України з імплантованим БЕН та запитів на формування сертифікатів ключів ЕЦП та шифрування Центр автоматично формує електронне підтвердження та передає його до РС ДМС.
11. Після отримання запитів на реєстрацію фізичної особи - власника паспорта громадянина України з імплантованим БЕН та запитів на формування сертифікатів ключів ЕЦП та шифрування, Центр здійснює відповідно реєстрацію особи у власному реєстрі підписувачів, перевірку унікальності відкритих ключів та якщо ключі унікальні формує сертифікати ключів ЕЦП і шифрування в автоматичному режимі.
12. Результат обробки запитів на реєстрацію фізичної особи - власника паспорта громадянина України з імплантованим БЕН та запитів на формування сертифікатів ключів ЕЦП та шифрування передається Центром до ВІС у вигляді повідомлень, які містять відповідно реєстраційний номер підписувача у реєстрі підписувачів Центру та відомості про чинність сформованих сертифікатів ключів ЕЦП та шифрування власника паспорта.
13. Публікація сформованих сертифікатів ключів ЕЦП та шифрування здійснюється автоматично на електронному інформаційному ресурсі Центру .
14. Початком строку дії особистих ключів вважається дата та час формування сертифікатів ключів ЕЦП та шифрування, що містять відкриті ключі відповідної пари ключів. Строк дії особистих ключів дорівнює строку чинності відповідних сертифікатів ключів.
15. Генерація чергових пар особистих та відкритих ключів для ЕЦП та шифрування здійснюється фізичною особою - власником паспорта громадянина України з імплантованим БЕН самостійно із використанням надійних засобів ЕЦП з дотриманням вимог інструкції щодо порядку генерації ключових даних і поводження (обліку, зберігання, знищення) з ключовими документами (далі – інструкція).
16. Надійні засоби ЕЦП з інструкціями до них надаються Центром шляхом передачі цих засобів на носіях інформації безпосередньо фізичній особі - власнику паспорта громадянина України з імплантованим БЕН або шляхом надання доступу через електронний інформаційний ресурс Центру. Надійні засоби ЕЦП можуть надаватись у вигляді окремих програмних додатків або програмних модулів (криптобібліотек), що функціонують у складі інших програмних додатків.
17. Центр та суб’єкти, що здійснюють представництво Центру, можуть надавати допомогу в генерації чергових пар особистих та відкритих ключів для ЕЦП та шифрування безпосередньо в офісах у разі їх особистого відвідування фізичними особами - власниками паспорта громадянина України з імплантованим БЕН.
18. Надійні засоби ЕЦП, що надаються Центром, повинні забезпечувати формування запитів на реєстрацію фізичної особи - власника паспорта громадянина України з імплантованим БЕН в якості підписувача, запитів на формування сертифікатів ключів ЕЦП та шифрування, а також відправку таких запитів до Центру для формування чергових сертифікатів ключів ЕЦП та шифрування.

Надійні засоби ЕЦП можуть надаватись фізичним особам - власникам паспорта громадянина України з імплантованим БЕН іншими суб’єктами правових відносин у сфері послуг ЕЦП за умов, що такі засоби ЕЦП мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації та є сумісними з програмним забезпеченням Центру.

1. Формування чергових сертифікатів ключів ЕЦП та шифрування за отриманими запитами здійснюється Центром автоматично. При цьому здійснюється скасування попередньо сформованих сертифікатів ключів.
2. У випадку закінчення строку дії паспорта громадянина України з імплантованим БЕН, його повернення державі, визнання недійсним та знищення засобами ВІС автоматично формується та відправляється до Центру запит на скасування діючих сертифікатів ключів ЕЦП та шифрування фізичної особи - власника паспорту. Після отримання запиту Центр здійснює скасування відповідних сертифікатів ключів та повертає ВІС повідомлення із зазначенням результату.
3. У випадку тимчасового вилучення паспорта громадянина України з імплантованим БЕН діючі сертифікати ключів ЕЦП та шифрування фізичної особи - власника паспорту можуть бути заблоковані на підставі заяви на блокування сертифікатів ключів, поданої до Центру підписувачем у порядку, передбаченому Регламентом роботи Центру.

З метою забезпечення захисту особистого ключа від компрометації підписувач - власник тимчасово вилученого паспорта громадянина України з імплантованим БЕН зобов’язаний не розголошувати та не повідомляти особам, якими вилучено паспорт, пароль доступу до особистого ключа (значення ПІН1(2) та ПАК1(2)) та ключову фразу для голосової автентифікації.

1. Після повернення підписувачу тимчасово вилученого паспорта громадянина України з імплантованим БЕН поновлення заблокованих сертифікатів ключів, строк чинності яких не закінчився, здійснюється за ініціативою підписувача на підставі поданої до Центру заяви на поновлення сертифікатів ключів у порядку, передбаченому Регламентом роботи Центру.

Якщо строк чинності сертифікатів ключів фізичної особи - власника паспорту закінчився, то генерація чергових пар особистих та відкритих ключів для ЕЦП та шифрування, формування чергових сертифікатів ключів здійснюється відповідно пунктів 25-29 цього Порядку.

1. Процедури блокування, поновлення та скасування сертифікатів ключів ЕЦП та шифрування в інших випадках, передбачених Законом України «Про електронний цифровий підпис», здійснюється у відповідності до Регламенту роботи Центру.
2. Захист персональних даних фізичних осіб - власників паспорта громадянина України з імплантованим БЕН здійснюється відповідно до законодавства у сфері захисту персональних даних.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_