**Вимоги**

**до захищених носіїв особистих ключів (ЗНОК)**

ЗНОК повинні бути сумісні з програмно-технічним комплексом «Клієнт Казначейства – Казначейство» та засобами електронного цифрового підпису, що використовуються у внутрішній платіжній системі Державної казначейської служби України, для роботи в операційних системах Microsoft Windows 2003/2008/7/8/10 та через WEB інтерфейс.

НКІ мають бути виготовлені за смарт-карт (SmartCard) технологіями, працювати під управлінням файлової операційної системи для мікропроцесорних карт і відповідати вимогам міжнародного стандарту ISO/IEC 7816.

НКІ мають підтримувати одночасне зберігання особистих ключів та апаратне виконання криптографічних перетворень згідно із стандартами: ДСТУ 4145-2002, ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, RSA, SHA-1; генерацію особистих ключових даних і формування електронного цифрового підпису (ЕЦП) відповідно до ДСТУ 4145-2002 з довжиною ключа 163 - 50біт та відповідно до PKCS#1 RSA Cryptography Standard з довжиною ключа 512 - 2048 біт. Всі криптографічні операції повинні виконуватись у захищеній пам’яті НКІ. Повинна забезпечуватись неможливість вилучення закритих ключів із пам’яті НКІ. Час формування ЕЦП відповідно до ДСТУ 4145-2002 з довжиною ключа 191 біт не повинен перевищувати 30 мс, з довжиною ключа 257 біт – 50 мс. Час формування ЕЦП відповідно до PKCS#1 RSA Cryptography Standard з довжиною ключа 2048 біт не повинен перевищувати 2000 мс.

Об’єм захищеної пам’яті ЗНОК має становити не менше 32 КБ.

Доступ до ЗНОК повинен бути захищений за допомогою ПІН-коду або паролю доступу.

Протокол взаємодії з ЗНОК повинен забезпечувати захист від модифікації даних і перехоплення секретних даних у каналі обміну між засобом КЕП і ЗНОК.

ЗНОК повинен використовувати алгоритм ДСТУ ГОСТ 28147:2009 в режимах гамування зі зворотним зв’язком та вироблення імітовставки для захисту даних у процесі обміну.

ЗНОК мають бути представлені у форм-факторі USB носіїв, реалізований USB v2.0 інтерфейс із ресурсом USB-з’єднувача не менше 5 000 з’єднань. ЗНОК мають відповідати стандарту Windows PC/SC та підтримувати Microsoft CCID.

Для ЗНОК має бути підтверджена наявність позитивного експертного висновку за результатами державної експертизи у сфері криптографічного захисту інформації.

ЗНОК має відповідати таким вимогам:

реалізація криптографічних алгоритмів повинна унеможливлювати сторонній доступ до ключової інформації та результатів проміжних розрахунків під час їх виконання;

реалізація генерації ключів для криптографічних алгоритмів повинна унеможливлювати сторонній доступ до ключової інформації та результатів проміжних розрахунків під час їх виконання.

|  |  |
| --- | --- |
|  |  |