Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03680,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

19.12.2013р № 05/02/02-4771

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 19.12.2013 м. Київ

Виданий: Товариству з обмеженою відповідальністю "ТЕХНОКОНСАЛТИНГ" (код ЄДРПОУ 25284317)

на підставі рішення Експертної комісії з питань проведення державної експертизи в сфері криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України, протокол від 19.12.2013 № 131.

Об'єкт експертизи: Програмно-технічний комплекс центру сертифікації ключів "TACSK" (804.25284317.00002-01 90 01).

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "ТЕХНОКОНСАЛТИНГ" (код ЄДРПОУ 25284317).

Експертний заклад: Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ" (код ЄДРПОУ 34979237).

Висновки:

1. В складі об'єкту експертизи можуть бути використані: Засіб електронного цифрового підпису апаратно-програмний "TELLIPSE" (ТУ У 30.0-25284317-001:2008), Засіб електронного цифрового підпису апаратно-програмний "TEllipseST" (ТУ У 30.0-25284317-002:2011), Засіб електронного цифрового підпису апаратно-програмний "TELLIPSE3" (ТУ У 26.1-25284317-003:2013).
2. Програмне забезпечення об'єкту експертизи використовує функції криптографічних перетворень, які реалізовані у виробах "TELLIPSE", "TEllipseST", "TELLIPSE3" (в частині формування особистого та відкритого ключів електронного цифрового підпису, а також формування електронного цифрового підпису), правильно.
3. В об'єкті експертизи криптографічні алгоритми реалізовані відповідно до вимог ГОСТ 34.311-95, ДСТУ 4145-2002.
4. Алгоритм генерації випадкових чисел, що реалізований в програмному забезпеченні об'єкта експертизи відповідає вимогам додатка А ДСТУ 4145-2002.
5. Алгоритм формування початкових значень генератора випадкових послідовностей, що реалізований в програмному забезпеченні об'єкта експертизи, відповідає документу "Методика ініціалізації генератора випадкових послідовностей" (804.25284317.00002 – 01 91 01).
6. Формат посиленого сертифіката відкритого ключа, структура об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами, формат списку відкликаних сертифікатів, протокол фіксування часу, протокол визначення статусу сертифіката, які реалізовані та використовуються в об'єкті експертизи, відповідають вимогам наказу Міністерства юстиції України та Адміністрації Держспецзв'язку від 20.08.2012 № 1236/5/453 "Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних

засобах електронного цифрового підпису", зареєстрованого в Міністерстві юстиції України 20.08.2012 за № 1398/21710.

7. Об'єкт експертизи відповідає вимогам технічного завдання на Програмно-технічний комплекс центру сертифікації ключів "TACSK" (804.25284317.00002-01 90 01) та Доповнення № 1 до нього (804.25284317.00002-01 90 02) в частині реалізації функцій криптографічних перетворень (п.4.2.1.5, 4.2.1.6, 4.2.2.6, 4.2.4.1 – 4.2.4.5, 4.2.4.7, 4.2.6.1).

8. Об'єкт експертизи може бути використаний для побудови акредитованих центрів сертифікації ключів.

Особливі умови (рекомендації):

Дія експертного висновку поширюється на зразки об'єкта експертизи, у яких криптографічні перетворення здійснюються програмними модулями, які мають наступні значення геш-функцій:

Nova.dll	66A27FF5 09BE02F8 48A0A631 810C1D06 84A7A45A 09A0AA96 762599A5 C0162180
TECCheck.dll	D4378AB9 99980C0D 23E09197 F5FA04B9 069B2E64 9DBCB874 C316C483 CF5FEDD8

Розрахунок геш-функцій здійснено відповідно до ГОСТ 34.311-95 з урахуванням значення нульового стартового вектора та ДКЕ № 1 з додатка № 1 до Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженої наказом Адміністрації Держспецзв'язку від 12.06.2007 № 114, зареєстрованої в Міністерстві юстиції України 25.06.2007 за № 729/13996.

Термін дії експертного висновку – до 19.12.2018.

Заступник Голови Служби О.В. Корнейко