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

05.04.2016 № 05/02/02-1422

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 05.04.2016 м. Київ

Виданий: Товариству з обмеженою відповідальністю "АЛТЕРСАЙН" (код ЄДРПОУ 38061489)

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 31.03.2016 № 234.

Об'єкт експертизи: Програмне забезпечення програмно-технічного комплексу центру сертифікації ключів "eSign" UA.36529128.00003-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "АЛТЕРСАЙН" (код ЄДРПОУ 38061489).

Експертний заклад: Товариство з обмеженою відповідальністю "БІЗТЕХ" (код ЄДРПОУ 36529128).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, які визначені ДСТУ ГОСТ 28147:2009 (в режимі гамування зі зворотним зв'язком), ГОСТ 34.311-95, ДСТУ 4145-2002 (при реалізації в поліноміальному базисі).
2. В об'єкті експертизи алгоритм генерації випадкових послідовностей відповідає вимогам додатку А ДСТУ 4145-2002.
3. В об'єкті експертизи алгоритм формування початкових значень генератора випадкових двійкових послідовностей відповідає вимогам документа "Методика формування початкових значень генератора випадкових двійкових послідовностей" UA.36529128.00003-01 91 01.
4. Формат посиленого сертифіката відкритого ключа, структура об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами, формат списку відкликаних сертифікатів, формат підписаних даних, протокол фіксування часу, протокол визначення статусу сертифіката, які реалізовані та використовуються в об'єкті експертизи, відповідають вимогам наказу Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.08.2012 № 1236/5/453 "Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису", зареєстрованого у Міністерстві юстиції України 20.08.2012 за № 1398/21710.
5. Формати криптографічних повідомлень, які реалізовані та використовуються в об'єкті експертизи, відповідають вимогам наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 "Про затвердження Вимог до форматів криптографічних повідомлень", зареєстрованого у Міністерстві юстиції України 14.01.2013 за № 108/22640.

6. Алгоритми формування ключів шифрування ключів та захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування, формати транспортних контейнерів особистих ключів електронного цифрового підпису та особистих ключів шифрування, формати контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів, прикладний програмний інтерфейс, які реалізовані, створюються та використовуються в об'єкті експертизи, відповідають вимогам спільного наказу Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 27.12.2013 № 2782/5/689 "Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису", зареєстрованого в Міністерстві юстиції України 27.12.2013 за № 2228/24759.
7. Об'єкт експертизи відповідає вимогам технічного завдання UA.36529128.00003-01 90 01 із Доповненням № 1 UA.36529128.00003-01 90 02, Доповненням № 2 UA.34979237.00003-01 90 03 до нього, в частині реалізації функцій криптографічних перетворень.
8. Об'єкт експертизи може бути використаний для криптографічного захисту інформації з обмеженим доступом (крім службової інформації та інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом.
9. Об'єкт експертизи може бути застосований 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, що мають наступні значення геш-функцій:

```
ESign.Crypto.Cms.dll  9DC7CF62 4DEBAACC 541DAD01 5C5C5D40 C6D5905D F5DE5F97 19E027F3 55E6B0A8
ESign.Crypto.Core.dll EABAD671 7C2629E9 1ECF3018 E2662C76 80FEA4FC 99694BEA 8AD135CA 98DE1E6D
ESign.Crypto.Ocsp.dll EB82059A B5082A3C 300F4124 9100362D 9EF16283 9C2DB47E B9C95539 CF011FC4
ESign.Crypto.Pkcs.dll EABB2F5E DC0C8633 AE3177B3 6E1E755B 028592F8 FA8AC47A EBE16BBD 471BAEF8
ESign.Crypto.Pkix.dll 2EFB5003 A10F77B2 BD22F8D0 B037D8BB FAA24D31 1588A5EA CC6FBA04 CDBF9339
ESign.Crypto.Tsp.dll  393229A2 ED6D7A9B E209D47D 8D672AC5 4A261D14 692F5E41 24BA211F FFF50572
```

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 Державної служби спеціального зв'язку та захисту інформації України від 12.06.2007 № 114, зареєстрованої в Міністерстві юстиції України 25.06.2007 за № 729/13996.

Термін дії експертного висновку – до 20.11.2020.

Перший заступник Голови Служби О.М. Чаузов