



ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03110,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

15.10.2019 № 04/03/02 - 2956

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 15.10.2019

м. Київ

Виданий: Товариству з обмеженою відповідальністю «ДІСІЕНСІ»
(код ЄДРПОУ 41564452)

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 10.10.2019 № 425.

Об'єкт експертизи: Програмний засіб «Бібліотека криптографічних перетворень АРТ-ЛІБ»
UA.41564452.00001-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю
«ДІСІЕНСІ» (код ЄДРПОУ 41564452).

Експертний заклад: Адміністрація Державної служби спеціального зв'язку та захисту
інформації України (код ЄДРПОУ 34620942).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002, ДСТУ 7564:2014, ДСТУ 7624:2014.
2. В об'єкті експертизи алгоритм генерації псевдовипадкових послідовностей відповідає додатку А ДСТУ 4145-2002.
3. В об'єкті експертизи правильно реалізовано протокол автономного узгодження ключів в групі точок еліптичної кривої типу Діффі-Геллмана (KANIDH), визначений п. 8.2 ДСТУ ISO/IEC 15946-3:2006.
4. В об'єкті експертизи алгоритм генерації та зберігання ключових даних відповідає документу «Методика захисту ключової інформації на зовнішніх носіях» UA.41564452.00001-01 ME 01.
5. В об'єкті експертизи алгоритм формування початкових значень генератора випадкових двійкових послідовностей відповідає документу «Методика ініціалізації генератора випадкових послідовностей» UA.41564452.00001-01 90 01.
6. 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.

7. Формати криптографічних повідомлень та протоколи розподілу ключів, 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 в Міністерстві юстиції України 14.01.2013 за № 108/22640.

8. Алгоритми формування ключів шифрування ключів та захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування, формати контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів, 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.

9. Формати запитів на формування сертифікатів, що створюються та обробляються об'єктом експертизи, відповідають вимогам PKCS#10 Certification Request Syntax Standard.

10. Об'єкт експертизи відповідає вимогам технічного завдання UA.41564452.00001-01 ТЗ-01 із Доповненням № 1 до нього в частині реалізації функцій криптографічних перетворень.

11. 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.

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:

Win32\COM\AMCrypto.dll	AFFE8B38	64AD7F07	539DC038	4F1074EB	374601F4	63B0A8F4	80D6A195	867C65C3
Win32\COM\BaseCrypt.dll	D7DDD139	F8469BCD	3B95CD7A	63EAE985	A5560476	AA7F20A2	59760CCC	FA47E0BA
Win32\COM\NKi.dll	34950C16	7AF0EC85	C4997FE1	83958BF0	B15F9383	857B0116	6793ABD6	D8D718F3
Win32\COM\Pkcs11.dll	A5108773	E1FA5695	E1C1EB07	7A9F1ED9	40DA41EA	D526B7A3	65EF15AD	998E36A0
Win32\COM\PKI.dll	6316A46E	9BC5B944	8D22F340	7E5346DC	86F4E098	E91F6B83	A3F14F94	7F89FCD3
Win32\NET\AMCryptoNET.dll	00BF06C7	91BB9E2B	1555395D	3F94750E	D647647C	1655557F	A6D35CEA	82A9DFD4
Win32\NET\BaseCrypt.dll	D7DDD139	F8469BCD	3B95CD7A	63EAE985	A5560476	AA7F20A2	59760CCC	FA47E0BA
Win32\NET\NKi.dll	34950C16	7AF0EC85	C4997FE1	83958BF0	B15F9383	857B0116	6793ABD6	D8D718F3
Win32\NET\Pkcs11.dll	A5108773	E1FA5695	E1C1EB07	7A9F1ED9	40DA41EA	D526B7A3	65EF15AD	998E36A0
Win32\NET\PKI.dll	6316A46E	9BC5B944	8D22F340	7E5346DC	86F4E098	E91F6B83	A3F14F94	7F89FCD3
Win64\COM\AMCrypto.dll	10D26243	442901B8	20E8DA00	8EBF5E8C	644F993D	B062D426	AD95B740	5B89512F
Win64\COM\BaseCrypt.dll	03DB77EA	9F60FB7D	6266BBE9	02F62E93	40BF1762	CE4ED496	6267CCFC	37CEA73B
Win64\COM\NKi.dll	45064FAA	3C85A328	C86834D1	18D751D8	72223B07	6F3642FE	7E1FA197	EF9C9D1D
Win64\COM\Pkcs11.dll	0F457915	57EE405A	3AB09826	7F21A6F1	BA4914B3	0CC475C6	10ADC2F3	D16454C2
Win64\COM\PKI.dll	55340426	2D5B634C	3F2091D7	4B513C88	AD7FA906	43963B02	BA87DB54	B52A88F0
Win64\NET\AMCryptoNET.dll	FE60472D	91D0E324	0771AF60	3D06E6E2	DDFE54C8	762A7B4A	1071DAA3	CDB0426A
Win64\NET\BaseCrypt.dll	03DB77EA	9F60FB7D	6266BBE9	02F62E93	40BF1762	CE4ED496	6267CCFC	37CEA73B
Win64\NET\NKi.dll	45064FAA	3C85A328	C86834D1	18D751D8	72223B07	6F3642FE	7E1FA197	EF9C9D1D
Win64\NET\Pkcs11.dll	0F457915	57EE405A	3AB09826	7F21A6F1	BA4914B3	0CC475C6	10ADC2F3	D16454C2
Win64\NET\PKI.dll	55340426	2D5B634C	3F2091D7	4B513C88	AD7FA906	43963B02	BA87DB54	B52A88F0

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 10.10.2024.

Перший заступник Голови Служби



Олександр ЧАУЗОВ