Прим. № 1

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

06.04.2018 № 04/03/02-1541

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 06.04.2018 м. Київ

Виданий: Товариству з обмеженою відповідальністю «ДБО Софт» (код ЄДРПОУ 37619243)

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 30.03.2018 № 336.

Об'єкт експертизи: Програмне забезпечення програмно-технічного комплексу центру сертифікації ключів «Integra CA» UA.37619243.00010.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «ДБО Софт» (код ЄДРПОУ 37619243).

Експертний заклад: Товариство з обмеженою відповідальністю «Українські технології безпеки» (код ЄДРПОУ 40421767).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009, ДСТУ 4145-2002, ГОСТ 34.311-95.
2. 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.
3. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений PKCS#1 v2.1 RSA Cryptography Standard (за схемами RSAES-OAEP, RSAES-PKCS1-v1_5).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису RSA, визначений PKCS#1 v2.1 RSA Cryptography Standard (за схемою RSASSA-PKCS1-v1_5).
6. В об'єкті експертизи алгоритм генерації ключових даних відповідає документу «Методика генерації ключових даних UA.37619243.00010-01 92 01-1».
7. 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, що 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.

8. Формати криптографічних повідомлень та протокол узгодження ключа Діффі-Геллмана ECDH, що 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.
9. Формати контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів, що реалізовані 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.
10. Об'єкт експертизи відповідає вимогам технічного завдання UA.37619243.00010-01 90 01-1 із Доповненням № 1 та Доповненням № 2 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.
12. Об'єкт експертизи може бути використаний для побудови акредитованого центру 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:

ICA-CA/lib/asn1-1.9.5.jar*	21a46543 708a1af2 1c96d5af d9a8e291 d040a719 78c82868 236b663a 45d64314
ICA-CA/lib/ca-server.jar*	3bbc8bf5 5b67a169 efe0e466 f27f9659 63908abb 39cc9e4c de45909d ee3ea902
ICA-CA/lib/cmp.jar*	2853946e 2fab925f a618ee9f a7683fd4 ccb8ba43 69a83603 cca971f8 a7101623
ICA-CA/lib/core.jar*	7f2d1e04 1d9d66b9 b2b56768 8f97893f 857eb843 948649c3 053b9486 a1d0044a
ICA-CA/lib/crypto-core-1.15.2.jar*	b1b55dfa 5c3b0912 4c633e58 8aeced00 4e83c2c1 ee34810c 78bf0e0b 3a20d743
ICA-CA/lib/integra-crypto-2.9.0.jar*	18346423 963b2f36 3c05426c f960ca91 659a6a90 b8ada85c 61c66ad7 a2eb4b33
ICA-CA/lib/pkix-1.38.5.jar*	a7176ca6 356ad1fb 4194722b 3813e43d d9f595b0 3e5aab94 4db0b803 b5ae104e
ICA-CA/lib/pkix-engine-1.2.4.jar*	8834f436 bb88d0b3 789dd97c 65e95536 05ddeef8 0ac641c1 1d7a3f9c e0378269
ICA-RA/lib/asn1-1.9.5.jar*	21a46543 708a1af2 1c96d5af d9a8e291 d040a719 78c82868 236b663a 45d64314
ICA-RA/lib/cmp.jar*	2853946e 2fab925f a618ee9f a7683fd4 ccb8ba43 69a83603 cca971f8 a7101623
ICA-RA/lib/core.jar*	7f2d1e04 1d9d66b9 b2b56768 8f97893f 857eb843 948649c3 053b9486 a1d0044a
ICA-RA/lib/crypto-core-1.15.2.jar*	b1b55dfa 5c3b0912 4c633e58 8aeced00 4e83c2c1 ee34810c 78bf0e0b 3a20d743
ICA-RA/lib/integra-crypto-2.9.0.jar*	18346423 963b2f36 3c05426c f960ca91 659a6a90 b8ada85c 61c66ad7 a2eb4b33
ICA-RA/lib/pkix-1.38.5.jar*	a7176ca6 356ad1fb 4194722b 3813e43d d9f595b0 3e5aab94 4db0b803 b5ae104e
ICA-RA/lib/pkix-engine-1.2.4.jar*	8834f436 bb88d0b3 789dd97c 65e95536 05ddeef8 0ac641c1 1d7a3f9c e0378269
ICA-RA/lib/ra-server.jar*	d8804ce3 059f4d20 6f6b3441 f6545722 161681d7 4b452d97 d5b03d2d 249cd51d
ICA-CA-WEB/lib/asn1-1.9.5.jar*	21a46543 708a1af2 1c96d5af d9a8e291 d040a719 78c82868 236b663a 45d64314
ICA-CA-WEB/lib/ca-web-server.jar*	e9e0215e 51016a8d 00d741d0 e6e2bc31 d7e7bf28 dfc00b90 95f5da22 de6a693b
ICA-CA-WEB/lib/core.jar*	7f2d1e04 1d9d66b9 b2b56768 8f97893f 857eb843 948649c3 053b9486 a1d0044a
ICA-CA-WEB/lib/pkix-1.38.5.jar*	a7176ca6 356ad1fb 4194722b 3813e43d d9f595b0 3e5aab94 4db0b803 b5ae104e

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 30.03.2023.

Перший заступник Голови Служби О.М. Чаузов