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

05.09.2018 № 04/03/02-3497

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 04.09.2018 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 04.09.2018 № 361.

Об'єкт експертизи: Програмний комплекс централізованої ідентифікації та електронного цифрового підпису «iSign» 804.25284317.00003.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «Техноконсалтинг» (код ЄДРПОУ 25284317).

Експертний заклад: Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ імені Ігоря Сікорського» (код ЄДРПОУ 34979237).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ 4145-2002 (у поліноміальному базисі), ГОСТ 34.311-95.
2. В об'єкті експертизи правильно реалізовано алгоритм формування та перевіряння електронного цифрового підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2015.
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений IEEE P1363-2000, PKCS#1 v2.2 RSA Cryptography Standard.
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES, визначений ДСТУ ISO/IEC 18033-3:2015 (в режимі CBC, визначеному ДСТУ ISO/IEC 10116:2015).
5. В об'єкті експертизи механізми ідентифікації користувачів, формування електронного цифрового підпису, шифрування даних, що передаються між об'єктом експертизи та веб-браузером користувача, а також захищеного зберігання паролів доступу користувачів контейнерів реалізовано відповідно до документу «Програмний комплекс централізованої ідентифікації та електронного цифрового підпису «iSign». Методика ідентифікації користувачів та формування електронного цифрового підпису 804.25284317.00003 – 01 91 01».
6. Формат посиленого сертифіката відкритого ключа, структура об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами, формат підписаних даних, 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 в Міністерстві юстиції України 20.08.2012 за № 1398/21710.

7. 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, інтерфейси засобів криптографічного захисту інформації, що 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.
8. Об'єкт експертизи відповідає вимогам технічного завдання 804.25284317.00003-01 90 01 в частині реалізації функцій криптографічних перетворень.
9. 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 програмним модулем, що має наступне значення геш-функції:

EUSignJawa.jar	6AEDD23F 137304E5 18897ADC EC494522 A3DD5FCB E706CD5E CBB60DB5 FDBCB8A1

Розрахунок геш-функції 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 04.09.2023.

Перший заступник Голови Служби О.М. Чаузов