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

08.12.15 № 05/02/02-5253

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 03.12.2015 м. Київ

Виданий: Товариству з обмеженою відповідальністю "АВТОР" (код ЄДРПОУ 32248356)

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 03.12.2015 № 220.

Об'єкт експертизи: Засоби електронного цифрового підпису "CryptoLibV2" АЧСА.467149.001, АЧСА.467149.002, АЧСА.767149.001-01, АЧСА.767149.002-01, АЧСА.767149.002-02.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "АВТОР" (код ЄДРПОУ 32248356).

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

1. В об'єкті експертизи криптографічні алгоритми реалізовано відповідно до вимог ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002.
2. В об'єкті експертизи правильно реалізовані криптографічні алгоритми шифрування DES, TDEA, AES (в режимах ECB, CBC, CFB, згідно розділу 9 ISO/IEC 10116:2006) відповідно до ISO/IEC 18033-3:2010.
3. В об'єкті експертизи правильно реалізований криптографічний алгоритм шифрування RSA який визначений в PKCS#1 v2.1 RSA Cryptography Standard (за схемою RSAES-PKCS1-v1_5).
4. В об'єкті експертизи правильно реалізований криптографічний алгоритм електронного цифрового підпису RSA, який визначений PKCS#1 v2.1 "RSA Cryptography Standard" (за схемою RSASSA-PKCSl-vl_5).
5. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-512 відповідно до ДСТУ ISO/IEC 10118-3:2005.
6. В об'єкті експертизи формати та структури даних реалізовані відповідно до вимог RFC 5652 "Cryptographic Message Syntax (CMS)", RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 2560 "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP).
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, 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 (зі змінами).

8. Формати криптографічних повідомлень, які реалізовані та використовуються в об'єкті експертизи, відповідають вимогам наказу Адміністрації Держспецзв'язку від 18.12.2012 № 739 "Про затвердження Вимог до форматів криптографічних повідомлень", зареєстрованого в Міністерстві юстиції України 14.01.2013 за № 108/22640.
9. Алгоритми формування ключів шифрування ключів та захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування, форматів транспортних контейнерів особистих ключів електронного цифрового підпису та особистих ключів шифрування, інтерфейсів бібліотек криптографічного захисту інформації, форматів контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування, які 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 ТЗ.АЧСА.460720.001-01 із Доповненням № 1, 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 у якості надійного засобу електронного цифрового підпису у складі акредитованих центрів сертифікації ключів.

Особливі умови (рекомендації): Дія експертного висновку поширюється на зразки об'єкта експертизи, які виготовлені відповідно до технічних умов ТУ У 26.2-32248356-019:2013 із Сповіщенням про зміну ТУ № 1 (АЧСА.05-2015).

Термін дії експертного висновку – до 03.12.2020.

Перший заступник Голови Служби О.М. Чаузов

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ * Ідентифікаційний код 34620942 *