Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

01034, м. Київ, вул. Паторжинського, 5/7,
тел. (044) 281-90-10, факс: (044) 226-26-83, e-mail: info@dsszzi.gov.ua

05.09.2012 № 05/02/02-3804

ЕКСПЕРТНИЙ ВИСНОВОК

Виданий: Товариству з обмеженою відповідальністю "Аладдін Сек'юріті Солюшенс" (код ЄДРПОУ 33495924)

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 05.09.2012 № 94.

Об'єкт експертизи: Апаратно-програмні вироби JaCarta JC142, JaCarta JC242, JaCarta JC342, JaCarta JC203.

Розроблений (виготовлений): Athena Smartcart Solutions, Inc. Японія.

Експертний заклад: Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ" (код ЄДРПОУ 34979237).

Висновки:

1. В об'єкті експертизи алгоритм шифрування відповідає вимогам алгоритму DES, визначеному в FIPS PUB 46-3.
2. В об'єкті експертизи алгоритм шифрування відповідає вимогам алгоритму TDES, визначеному в п. 4.1 ISO/IEC 18033-3:2010.
3. В об'єкті експертизи алгоритм гешування відповідає вимогам алгоритму AES, визначеному в п. 5.1 ISO/IEC 18033-3:2010.
4. В об'єкті експертизи алгоритми гешування відповідають вимогам алгоритмів SHA-1, визначений в розділі 9 ДСТУ ISO/IEC 10118-3:2005, SHA-256, визначений в розділі 10 ДСТУ ISO/IEC 10118-3:2005, SHA-384, визначений в розділі 12 ДСТУ ISO/IEC 10118-3:2005, SHA-512, визначений в розділі 11 ДСТУ ISO/IEC 10118-3:2005.
5. В об'єкті експертизи алгоритм гешування відповідає вимогам алгоритму ГОСТ 34.311-95.
6. В об'єкті експертизи алгоритм шифрування, формування та перевіряння електронного цифрового підпису інформації відповідає вимогам алгоритму RSA, визначений в IETF RFC 3447 (у варіанті RSASSA-PKCS1-v1_5).
7. В об'єкті експертизи алгоритм формування та перевіряння електронного цифрового підпису, відповідає вимогам ДСТУ 4145-2002.
8. Об'єкт експертизи відповідає умовам п. b) криптографічної примітки 3 позиції 5.A.2, п 1, 2 технічної примітки розділу 5 частини 2 додатку 1 до Порядку здійснення державного контролю за міжнародними передачами товарів подвійного використання, затвердженого Постановою Кабінету Міністрів України від 28.01.2004 № 86.

Особливі умови (рекомендації): Дія експертного висновку поширюється на зразки об'єкта експертизи JaCarta JC142 (№ 0950000439350497), JaCarta JC242 (№ A006745), JaCarta JC342 (№ 52000341229243), JaCarta JC203 (згідно з митною декларацією ВМД 125120105/2012/252367).

Термін дії експертного висновку: до 05.09.2015.

Перший заступник Голови Служби О.Г. Цуркан