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

13.05.2019 № 04/03/02-1282

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 13.05.2019 м. Київ

Виданий: Приватному акціонерному товариству «Інститут інформаційних технологій» (код ЄДРПОУ 22723472)

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 10.05.2019 № 400.

Об'єкт експертизи: Ключ електронний «Алмаз-1К» ЄААД.469535.153.

Розроблений (виготовлений): Приватним акціонерним товариством «Інститут інформаційних технологій» (код ЄДРПОУ 22723472).

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 (у режимах простої заміни, гамування зі зворотним зв'язком та вироблення імітовставки), ГОСТ 34.311-95, ДСТУ 4145-2002.
2. В об'єкті експертизи вимоги профілів захисту для пристроїв створення безпечного підпису реалізовані згідно ДСТУ EN 419211-1:2016 та ДСТУ EN 419211-2:2016.
3. В об'єкті експертизи алгоритм генерації випадкових двійкових послідовностей та порядок генерації ключових даних реалізовано згідно документу «Методика генерації ключових даних ЄААД.468244.020 Д1.05».
4. В об'єкті експертизи внутрішній апаратний генератор випадкових послідовностей реалізовано згідно документу «Методика генерації ключових даних ЄААД.468244.020 Д1.05».
5. Протокол взаємної автентифікації об'єкта експертизи з програмним забезпеченням користувачів відповідає документу «Методика (протокол) автентифікації програмних засобів користувачів та електронного ключа ЄААД.469535.153 Д3».
6. 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.
7. Об'єкт експертизи забезпечує захист записаних на нього даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.
8. В об'єкті експертизи криптографічний динамічний механізм узгодження ключів («Ephemeral-Static mode») реалізовано відповідно до вимог 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. 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 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.

10. Формати криптографічних повідомлень, що реалізовані 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.

11. Реалізовані в об'єкті експертизи інтерфейси, відповідають вимогам 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.

12. Об'єкт експертизи відповідає вимогам технічного завдання ЄААД.469535.153.01 ТЗ із Доповненням № 1 до нього, в частині реалізації функцій криптографічних перетворень.

13. Об'єкт експертизи може бути використаний в якості засобу кваліфікованого електронного підпису чи печатки для надання кваліфікованих електронних довірчих послуг.

14. 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, виготовлені відповідно до технічних умов ТУ У 26.2-22723472-020:2014 із Зміною № 1:2019 до них.

Термін дії експертного висновку – до 10.05.2024.

Голова Служби Л.О. Євдоченко