АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-92-10, факс: (044) 281-94-83,
e-mail: info@dsszzi.gov.ua, сайт: www.dsszzi.gov.ua, код згідно з ЄДРПОУ 34620942

29.07.2022 № 04-702/ВС1 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 29.07.2022 м. Київ

Виданий: Товариству з обмеженою відповідальністю «СПЕЦІНФОСИСТЕМИ» (код ЄДРПОУ 32436187)

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 27.07.2022 № 553.

Об'єкт експертизи: Ключ електронний «DIAMOND» 32436187.00001-01.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «СПЕЦІНФОСИСТЕМИ» (код ЄДРПОУ 32436187).

Експертний заклад: Товариство з обмеженою відповідальністю «АЛЬТАЇР-775» (код ЄДРПОУ 25197618).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ 7624:2014 (у режимах Калина-128/128-ECB, Калина-128/128-CTR, Калина-128/128-CFB, Калина-128/128-CBC,Калина-128/128-OFB, Калина-128/128-GCM, Калина-128/128-KW, Калина-128/256-ECB, Калина-128/256-CTR, Калина-128/256-CFB, Калина-128/256-CBC, Калина-128/256-OFB, Калина-128/256-GCM, Калина-128/256-KW, Калина-256/256-ECB,Калина-256/256-CTR, Калина-256/256-CFB, Калина-256/256-CBC, Калина-256/256-OFB, Калина-256/256-GCM, Калина-256/256-KW, Калина-256/512-ECB, Калина-256/512-CTR, Калина-256/512-CFB, Калина-256/512-CBC, Калина-256/512-OFB, Калина-256/512-GCM, Калина-256/512-KW, Калина-512/512-ECB, Калина-512/512-CTR, Калина-512/512-CFB, Калина-512/512-CBC, Калина-512/512-OFB, Калина-512/512-GCM, Калина-512/512-KW, ДСТУ 7564:2014 (у режимах Купина-256, Купина-384, Купина-512), ДСТУ 4145-2002 (у поліноміальному базисі), ГОСТ 28147-89 (у режимі простої заміни, гамування, гамування зі зворотним зв'язком та обчислення імітовставки), ГОСТ 34.311-95.

2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES, визначений ДСТУ ISO/IEC 18033-3:2015 (у режимах ECB, CTR, CFB, CBC, OFB згідно ДСТУ ISO/IEC 10116:2019 та у режимі GCM згідно NIST SP 800-38D, з довжиною ключа 128, 192, 256 біт).

3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений ДСТУ ISO/IEC 18033-2:2015 (за схемою RSAES-OAEP, з довжиною ключа 1024, 2048, 4096 біт).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм електронного підпису RSA, визначений ДСТУ ISO/IEC 14888-2:2015, PKCS#1 v.2.2 «RSA Cryptography Standard» (за схемами RSASSA-PKCS1-v1_5, RSASSA-PSS).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм обчислення та перевіряння електронного підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019 (до 521 біт в простому полі та до 571 біт в розширеному полі).
6. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
7. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-3-256, SHA-3-384, SHA-3-512, визначені ISO/IEC 10118-3:2018.
8. В об'єкті експертизи правильно реалізовано протокол автономного узгодження ключів в групі точок еліптичної кривої типу Діффі-Геллмана, визначений п. Е.7 додатку Е ДСТУ ISO/IEC 11770-3:2015 (до 521 біт в простому полі та до 571 біт в розширеному полі).
9. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування коду автентифікації повідомлень CBC-MAC за алгоритмом AES, визначений ДСТУ ISO/IEC 9797-1:2015, NIST SP-800-38A.
10. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування коду автентифікації повідомлень HMAC, визначений ДСТУ 9797-2:2015.
11. В об'єкті експертизи генерація, розподіл та зберігання ключових даних здійснюється відповідно до вимог документу «Методика генерації, розподілу та зберігання ключових даних UA.32436187.00001-01 90 02».
12. В об'єкті експертизи ініціалізація генератора псевдовипадкових послідовностей здійснюється відповідно до вимог документу «Методика ініціалізації генератора псевдовипадкових послідовностей UA.32436187.00001-01 90 01».
13. Методи захисту, реалізовані в об'єкті експертизи, відповідають вимогам до засобів криптографічного захисту інформації класу Б1 (захист від порушника другого рівня), визначеним в Положенні про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141, зареєстрованим в Міністерстві юстиції України 30.07.2007 за № 862/14129.
14. Об'єкт експертизи відповідає вимогам технічного завдання UA.32436187.00001-01 ТЗ 02 в частині реалізації функцій криптографічних перетворень.
15. Об'єкт експертизи може бути використаний як складова частина при побудові засобів криптографічного захисту інформації видів «А» та «Б», призначених 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 72.2-32436187-001:2022.

Термін дії експертного висновку – до 27.07.2027.

Голова Служби Юрій ЩИГОЛЬ