Прим. № 1

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@cip.gov.ua, сайт: www.cip.gov.ua, код згідно з ЄДРПОУ 34620942

21.08.2022 № 04-1017/ДСІ На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 21.08.2022 м. Київ

Виданий: Товариству з обмеженою відповідальністю «БАЗИС» (код ЄДРПОУ 31085786)

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 18.08.2022 № 555.

Об'єкт експертизи: Програмний виріб криптографічного захисту інформації Криптографічний сервіс-провайдер «Цезаріс-CSP-JM» 31085786.1КЦ.019.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «БАЗИС» (код ЄДРПОУ 31085786).

Експертний заклад: Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації (код ЄДРПОУ 34732331).

Висновки:
1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ 7564:2014 (для повідомлень кратних байту), ДСТУ 7624:2014 (для повідомлень кратних байту), ДСТУ 4145-2002.
2. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ГОСТ 28147-89 (у режимах простої заміни, гамування, гамування зі зворотним зв'язком та обчислення імітовставки), ГОСТ 34.311-95 (для повідомлень кратних байту).
3. В об'єкті експертизи алгоритм генерації випадкових двійкових послідовностей відповідає додатку А ДСТУ 4145-2002.
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений ДСТУ ISO/IEC 18033-2:2015, IETF RFC3447 (за схемами RSAES-OAEP, RSAES-PKCS1-v1_5).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису RSA, визначений ДСТУ ISO/IEC 14888-2:2015, IETF RFC3447 (за схемами RSASSA-PKCSl-vl_5, RSASSA-PSS).

6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019.
7. В об'єкті експертизи правильно реалізовано криптографічні алгоритми шифрування DES, TDEA, AES, визначені ДСТУ ISO/IEC 18033-3:2015 (у режимах ECB, OFB, CFB, CBC, CTR, визначених ДСТУ ISO/IEC 10116:2019).
8. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
9. 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.
10. В об'єкті експертизи правильно реалізовано криптографічний алгоритм генерації псевдовипадкових чисел HMAC-DRBG, визначений ДСТУ ISO/IEC 18031:2015.
11. Формат та вміст статусів сертифікатів та запитів на їх отримання, що реалізовані в об'єкті експертизи відповідає вимогам IETF RFC 6960 «Internet Public Key Infrastructure Online Certificate Status Protocol».
12. Формат та вміст сертифікатів і списків відкликаних сертифікатів, що реалізовані в об'єкті експертизи відповідають вимогам ДСТУ ETSI EN 319 412:2016 (ETSI EN 319 412:2016, IDT) «Електронні підписи й інфраструктури (ESI). Профілі сертифікатів».
13. Формат та вміст підписаних даних (криптографічних повідомлень типу «signed-data»), що реалізовані в об'єкті експертизи відповідають вимогам ДСТУ ETSI EN 319 122:2016 (ETSI EN 319 122:2016, IDT) «Електронні підписи й інфраструктури (ESI). Цифрові підписи CAdES».
14. Формат та вміст позначок часу TSP та запитів на їх отримання, що реалізовані в об'єкті експертизи відповідають вимогам ДСТУ ETSI EN 319 422:2016 (ETSI EN 319 422:2016, IDT). «Електронні підписи й інфраструктури. Протокол мітки часу та профілі токенів мітки часу».
15. В об'єкті експертизи формат файлу для зберігання ключової пари відповідає вимогам PKCS#12.
16. Алгоритми генерації та розподілу ключових даних, що реалізовано в об'єкті експертизи, відповідає вимогам документу «Методика генерації та розподілу ключових даних 31085786.1КЦ.019.М1.01.1».
17. Методи захисту, реалізовані в об'єкті експертизи, відповідають вимогам до засобів криптографічного захисту інформації класу В2 (захист від порушника першого та нульового рівнів), 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.
18. Об'єкт експертизи відповідає вимогам технічного завдання 31085786.1КЦ.019.ТЗ.01.1 в частині реалізації функцій криптографічних перетворень.
19. 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.
20. Об'єкт експертизи може бути використаний для надання кваліфікованих електронних довірчих послуг.

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи, у яких криптографічні перетворення здійснюються програмними модулями, значення геш-функцій яких наведено в додатку до цього експертного висновку, який є невід'ємною його частиною.

Термін дії експертного висновку – до 18.08.2027.

Голова Служби Юрій ЩИГОЛЬ