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

21.07.2021 № 04/05/01-2096 На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 21.07.2021 м. Київ

Виданий: Товариству з обмеженою відповідальністю «С.І.Т» (код ЄДРПОУ 38773869)

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 21.07.2021 № 508.

Об'єкт експертизи: Засіб криптографічного захисту інформації «3DA CA CLIENT».

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «С.І.Т» (код ЄДРПОУ 38773869).

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-CMAC, Калина-128/128-CBC, Калина-128/128-OFB, Калина-128/128-GCM, Калина-128/128-GMAC, Калина-128/128-CCM, Калина-128/128-XTS, Калина-128/128-KW, Калина-128/256-ECB, Калина-128/256-CTR, Калина-128/256-CFB, Калина-128/256-CMAC, Калина-128/256-CBC, Калина-128/256-OFB, Калина-128/256-GCM, Калина-128/256-GMAC, Калина-128/256-CCM, Калина-128/256-XTS, Калина-128/256-KW, Калина-256/256-ECB, Калина-256/256-CTR, Калина-256/256-CFB, Калина-256/256-CMAC, Калина-256/256-CBC, Калина-256/256-OFB, Калина-256/256-GCM, Калина-256/256-GMAC, Калина-256/256-CCM, Калина-256/256-XTS, Калина-256/256-KW, Калина-256/512-ECB, Калина-256/512-CTR, Калина-256/512-CFB, Калина-256/512-CMAC, Калина-256/512-CBC, Калина-256/512-OFB, Калина-256/512-GCM, Калина-256/512-GMAC, Калина-256/512-CCM, Калина-256/512-XTS, Калина-256/512-KW, Калина-512/512-ECB, Калина-512/512-CTR, Калина-512/512-CFB, Калина-512/512-CMAC, Калина-512/512-CBC, Калина-512/512-OFB, Калина-512/512-GCM, Калина-512/512-GMAC, Калина-512/512-CCM, Калина-512/512-XTS, Калина-512/512-KW), ДСТУ 7564:2014 (у режимах Купина-256, Купина-512), ДСТУ 8845:2019 (у режимах СТРУМОК-256, СТРУМОК-512), ГОСТ 34.311-95, ДСТУ 4145-2002.

2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES визначений ДСТУ ISO/IEC 18033-3:2015 (у режимах ECB, CBC, CFB, OFB, CTR, згідно ДСТУ ISO/IEC 10116:2019, у режимі CCM згідно NIST SP 800-38C, у режимі GCM згідно NIST SP 800-38D, у режимі KW згідно NIST SP 800-38F).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування TDEA визначений ДСТУ ISO/IEC 18033-3:2015 (у режимах ECB, CBC, CFB, OFB, CTR, згідно ДСТУ ISO/IEC 10116:2019).
4. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, WHIRLPOOL, RIPEMD-128, RIPEMD-160 визначені ДСТУ ISO/IEC 10118-3:2005.
5. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA3-224, SHA3-256, SHA3-384, SHA3-512, SM3, STREEBOG-256, STREEBOG-512, визначені ISO/IEC 10118-3:2018.
6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм гешування SHA-224 визначений IETF RFC 3874.
7. В об'єкті експертизи правильно реалізовано криптографічний алгоритми гешування MD5, визначений IETF RFC 1321 «The MD5 Message-Digest Algorithm».
8. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019.
9. В об'єкті експертизи правильно реалізовано криптографічний алгоритм електронного підпису RSA, визначений ДСТУ ISO/IEC 14888-2:2015 (за схемою RSASSA-PSS).
10. 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.
11. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений IETF RFC 8017 (за схемами RSAES-PKCS1-v1.5, RSAES-OAEP).
12. В об'єкті експертизи правильно реалізовано криптографічний алгоритм генерації псевдовипадкових чисел HMAC-DRBG відповідно до ДСТУ ISO/IEC 18031:2015.
13. В об'єкті експертизи правильно реалізовано механізм обчислення кодів автентифікації HMAC, визначений ДСТУ ISO/IEC 9797-2:2015.
14. В об'єкті експертизи правильно реалізовано формати сертифікатів та списків відкликаних сертифікатів, визначені ДСТУ ISO/IEC 9594-8:2014.
15. В об'єкті експертизи правильно реалізовано формат позначки часу, визначений ДСТУ ISO/IEC 18014-1:2015.
16. В об'єкті експертизи правильно реалізовано формат даних інтерактивного визначення статусу сертифіката, визначений IETF RFC 6960.
17. В об'єкті експертизи правильно реалізовано формат підписаних даних, визначений ДСТУ ETSI TS 101 733:2017.
18. В об'єкті експертизи правильно реалізовано формат криптографічних повідомлень, визначений IETF RFC 5652.
19. В об'єкті експертизи правильно реалізовано формат контейнерів ключів, визначений IETF RFC 7292.
20. В об'єкті експертизи правильно реалізовано шифрування ключової інформації в контейнерах ключів, визначене IETF RFC 8018.
21. В об'єкті експертизи генерація та розподіл ключових даних здійснюється згідно вимог документу «Методика генерації та розподілу ключових даних UA.38773869.00002-01 93 01».
22. В об'єкті експертизи ініціалізація генератора псевдовипадкових чисел здійснюється згідно вимог документу «Методика ініціалізації генератора псевдовипадкових чисел UA.38773869.00002-01 90 01».

23. 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 (зі змінами).
24. Об'єкт експертизи відповідає вимогам технічного завдання UA.38773869.00002-01 ТЗ 02 в частині реалізації функцій криптографічних перетворень.
25. 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, у яких криптографічні перетворення здійснюються програмними модулями, що мають наступні значення геш-функцій:

Windows x86	
uapkic.dll	E222EE14 4C595A21 7957A328 4B137170 208F882C E320742E 002D1EE6 871A9E9F
uapkif.dll	1BDE82F4 40B541F4 BD978197 D2DE9BE5 4885CBA5 EA52324F 2EFCBE7D 6F5F2C3A
Windows x86-64	
uapkic.dll	A8115B17 54EF5CBB 713DE1FE D8C1DAC4 641D83A4 1E476075 62A7F923 D354C822
uapkif.dll	D7B6F2D2 61B0F9A7 9C91396A 533899A3 48C907E2 12301A86 A1C0A274 3352920D
Linux x86-64	
libuapkic.so.2.0.0	B44B855E 06674515 6DE40808 EEBEBCC5 69D76C29 1D01CC78 AB925E79 B95BFDE7
libuapkif.so.2.0.0	2FC50317 E8DC9BFE FFDE97A1 FD3DEFA1 265B5A8A AE711B43 E4675D4B 5389C97E
Linux armv7	
libuapkic.so.2.0.0	D7DC3087 65DED669 94A373B2 C9282F17 3C83697C 372FB91F 0404F569 5B8733AA
libuapkif.so.2.0.0	6C0062E9 3F4F9F15 973E205F 9440E75C 795E9D3C 88F19822 DF09DA8C 465F4FC1
Linux armv8	
ibuapkic.so.2.0.0	A354844E 0CDF250B 8DCDA07C A4118E86 526CE082 9A131EC5 0BD904FB 2C75FF69
libuapkif.so.2.0.0	8BF5D310 A3608547 F7F672DD 84391F11 35575515 BABA72FF E26B94F7 3B77A046
Android x86-64	
libuapkic.so	8C6501A4 9B8A414C 233FD0BF D781D3F1 9F1A2520 8B6EC874 89C745CA 1B41E5F5
libuapkif.so	3CBF3996 200882CA 8F541426 937C5C99 76B3E595 1F8C3B42 5F3C7912 76BCBB44
Android armv8	
libuapkic.so	161AB3A1 2471B4AD AA728C55 E9E9808F 2CA70071 7CD40721 811A1D14 558DB7F2
libuapkif.so	6ED63601 DF95B3B5 23F2E15E 3D9BFEE3 5CB39CB1 C7E0F6D7 62645B7D 909DF060
FreeBSD x86-64	
libuapkic.so.2.0.0	E75C5180 E9CAE42A E8BA9C37 460F4C82 70DF7BBB 2ADC4471 3E0607AC 2D8EF165
libuapkif.so.2.0.0	8691BF42 55044D82 DE56BA00 8B3356A7 F58B1C04 53157529 10D0ED8A CFF6AED9
FreeBSD armv8	
libuapkic.so.2.0.0	693D6E7C 8585C235 B2EB0333 27F65C47 AEBFED90 083D3228 C3548023 D29D6EA9
libuapkif.so.2.0.0	9DECBE8A 3AA37A41 FCA7061F 8A07B0F0 9A7C38A4 FA03C94B DC44A2B2 5B8D59AE
iOS armv8	
libuapkic.2.0.0.dylib	900E1416 8FEA5382 6E7FF839 57D5B23F B1DCCE0F 3740F535 1CFEA4B1 DD32CABA
libuapkif.2.0.0.dylib	6B111EB8 9312E54C F21DA1EC 6E606C75 8C673787 1161C569 BF64E075 18F71DB8

MacOS x86-64

libuapkic.2.0.0.dylib	B45A7365 9F173CDD 203B9920 2F3D6A79 2E3B2FD7 DA9E1CDC 25877258 3C3042F7
libuapkif.2.0.0.dylib	FB78CCC6 704238C1 A1EC4339 03874A46 0E19D726 BDEE233B A157751C B47B530C

MacOS armv8

libuapkic.2.0.0.dylib	73F0CF01 9533A845 7869F4D0 F4243D96 3A48BCBD 6112E81D EDAE89E0 26913656
libuapkif.2.0.0.dylib	03F558A2 4793F964 98B0472A 2E6E8732 DABC43AF 48BD44F0 C64B3F52 93D995FE

Розрахунок геш-функцій здійснено відповідно до ГОСТ 34.311-95 з урахуванням значення нульового стартового вектора та ДКЕ № 1 з додатка № 1 до Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженої наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12.06.2007 № 114, зареєстрованої в Міністерстві юстиції України 25.06.2007 за № 729/13996.

Термін дії експертного висновку – до 21.07.2026.

Голова Служби Юрій ЩИГОЛЬ