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 № 04-1022/ВСІ На № _____ від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 21.08.2022 м. Київ

Виданий: Товариству з обмеженою відповідальністю «САЙФЕР ПРО» (код ЄДРПОУ 42125815)

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 комплекс криптографічних перетворень «Шифр+», версія 2.1 ТЗ У 72.2 23154898 003:2016.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «САЙФЕР ПРО» (код ЄДРПОУ 42125815).

Експертний заклад: Товариство із обмеженою відповідальністю «ЗАХИСТ.ЮЕЙ» (код ЄДРПОУ 42292899).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ 7564:2014, ДСТУ 7624:2014 (у режимах ECB, OFB, CFB, CBC, CTR, XTS, KW, CMAC, GMAC, GCM, CCM), ДСТУ 8845:2019, ДСТУ 9041:2020, ДСТУ 4145-2002 (у поліноміальному базисі).
2. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ГОСТ 28147-89 (у режимах простої заміни, гамування, гамування із зворотнім зв'язком та обчислення імітовставки), ГОСТ 34.311-95.3. В об'єкті експертизи алгоритми генерації випадкових двійкових послідовностей відповідають додатку А ДСТУ 4145-2002, NIST SP 800-90A rev.1, Intel Digital Random Number Generator (DRNG): Software Implementation Guide, Revision 1.1.
4. 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, CMAC, визначених ДСТУ ISO/IEC 10116:2019).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений ДСТУ ISO/IEC 18033-2:2015, IEEE P1363-2000, x9.31, PKCS#1 v1.5, PKCS#1 v2.2.
6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019, IEEE P1363-2000, NIST FIPS 186-4:2013.

7. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису EC-GDSA, визначений ДСТУ ISO/IEC 14888-3:2019, BSI-TR-03111:2012.
9. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису RSA (RSA1S, RSA2S), визначений ДСТУ ISO/IEC 14888-2:2015, IEEE P1363-2000, NIST FIPS 186-4:2013, x9.31.
10. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису EdDSA, визначений IETF RFC 8032.
11. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
12. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-224, SHA-512/224, SHA-512/256, визначені FIPS PUB 180-4:2012.
13. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-3/224, SHA-3/256, SHA-3/384, SHA-3/512, SHAKE128, SHAKE256, визначені NIST PUB 202.
14. В об'єкті експертизи правильно реалізовано алгоритми вироблення ключа шифрування на основі спільного секрету KDF1, KDF2, KDF3, визначені ДСТУ ISO/IEC 18033-2:2015.
15. В об'єкті експертизи правильно реалізовано алгоритми вироблення ключа шифрування на основі паролю PBKDF1, PBKDF2, визначені PKCS#5 v2.1, IETF RFC 2898.
16. В об'єкті експертизи правильно реалізовано алгоритм шифрування на основі паролю PBES2, визначений PKCS#5 v2.1, IETF RFC 2898.
17. В об'єкті експертизи правильно реалізовано алгоритм обчислення коду автентифікації на основі паролю PBMAC1, визначений PKCS#5 v2.1, IETF RFC 2898.
18. В об'єкті експертизи правильно реалізовано криптографічні протоколи розподілу ключів: ECKAS-DH1 (KANIDH, ECDH), визначені IEEE P1363-2000, ДСТУ ISO/IEC 11770-3:2015, NIST SP 800-56A Rev.3; ECKAS-DH2 (KADH2KP), визначені IEEE P1363-2000, ДСТУ ISO/IEC 11770-3:2015; ECKAS-MQV1 (KAMQV1P, KAMQV2P), визначені ДСТУ ISO/IEC 11770-3:2015, NIST SP 800-56A Rev.3; ECKAS-MQV2, визначені ДСТУ ISO/IEC 11770-3:2015; ECKAS-EG (KAEG), визначені ДСТУ ISO/IEC 11770-3:2015.
19. В об'єкті експертизи правильно реалізовано алгоритми обчислення коду автентифікації повідомлення з використанням: блокових симетричних шифрів ГОСТ 28147-89, ДСТУ 7624:2014, AES, DES, TDEA і геш-функцій, визначених ГОСТ 34.311-95, ДСТУ 7564:2014, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA-3/224, SHA-3/256, SHA-3/384, SHA-3/512, SHAKE128, SHAKE256, визначених IETF RFC 2104.
20. В об'єкті експертизи правильно реалізовано алгоритми кодування даних: EMSA1, визначені IEEE P1363-2000; EMSA2, визначені IEEE P1363-2000; EMSA3 визначені IEEE P1363-2000, PKCS#1 v2.2; EMSA4, визначені IEEE P1363-2000, PKCS#1 v2.2; EMSR1, визначені IEEE P1363-2000, ISO/IEC 9796:1991; EMSR3, визначені IEEE P1363a-2004, EME1, визначені IEEE P1363-2000, PKCS#1 v2.2, EME2, визначені PKCS#1 v2.2, EME-ДСТУ 9041:2020, визначені ДСТУ 9041:2020.
21. В об'єкті експертизи алгоритм ініціалізації генераторів випадкових послідовностей відповідає вимогам документа «Методика ініціалізації генератора випадкових двійкових послідовностей UA.33349855.00001 – 01 94 01».
22. 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.
23. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ У 72.2 23154898 003:2016 із доповненням № 1 до нього ТЗ У 72.2 42125815 001:2022 в частині реалізації функцій криптографічних перетворень.

24. 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:

Каталог android	
Каталог arm64-v8a	
libCCPPLib.a	CA4DE08C 2E253D84 8FB4BCF5 DA21FDA1 345E5044 05F4CE8B 08E0510B 2769DDBB
libCCPPLib.so	6972AE1F 2AFFE608 652591D5 3145A6F4 3EEED47D F2FF63FF C1599F7E 6D24DB74
Каталог armeabi-v7a	
libCCPPLib.a	85A7D341 383FB925 7141745C 6BE01DEA 313FBFCC 3E624FF1 7991B1C3 A6298497
libCCPPLib.so	B8274AA9 36A8B28C 4C0445C5 027D591D A5675B40 4346B05B 14F09E64 4FB84CD0
Каталог x86-64	
libCCPPLib.a	13524F54 34874316 9A118529 05799889 5B1C481E FB2E52AB 87592FD3 7362E08B
libCCPPLib.so	8EC7FC23 434DAE00 9D075D29 AB16131C 3FA2F9CB 494A9E5E 8863203B 091360FE
Каталог x86	
libCCPPLib.a	9408EBF5 358B5B1E 48A62418 1141D6F6 23102BA2 9296E965 C5BB970B 73C3DFF3
libCCPPLib.so	438F71D2 816982FE 6C56A6C2 45D54683 B9121B8E 4EB39A4E E1AD0CA5 3B86BF48
Каталог iOS	
libCCPPLib-iOS-static-arm64.a	E11F8BB1 7CF18AF2 EF372E05 C01EE812 D8F598DD 93B93C48 CBCB043E ACC75FD5
Каталог iOS-simulator	
libCCPPLib-iOS-static-x86-64.a	4FCC4ECA 7A1297DF 92B15E26 42E6BFE2 CEBD8774 63D374DC 4DC67FE3 E262B3B2
Каталог linux	
Каталог x86-64	
Каталог Release-DLL-x64-cannonlake	
libCCPPLib-linux.so	C32735E3 A54942EE F9B35F6C 52145F6B 183CD15D D63C06EA 128ECF9C 5893C3ED
Каталог Release-DLL-x64-cascadelake	
libCCPPLib-linux.so	C32735E3 A54942EE F9B35F6C 52145F6B 183CD15D D63C06EA 128ECF9C 5893C3ED
Каталог Release-DLL-x64-cooperlake	
libCCPPLib-linux.so	C32735E3 A54942EE F9B35F6C 52145F6B 183CD15D D63C06EA 128ECF9C 5893C3ED
Каталог Release-DLL-x64-generic	
libCCPPLib-linux.so	BCEB632B 50A256B8 96603D52 87556D15 5EA4AA63 E505688B 1CB40704 61E78D71
Каталог Release-DLL-x64-icelake-client	
libCCPPLib-linux.so	C32735E3 A54942EE F9B35F6C 52145F6B 183CD15D D63C06EA 128ECF9C 5893C3ED
Каталог Release-DLL-x64-icelake-server	
libCCPPLib-linux.so	C32735E3 A54942EE F9B35F6C 52145F6B 183CD15D D63C06EA 128ECF9C 5893C3ED
Каталог Release-DLL-x64-skylake-avx512	
libCCPPLib-linux.so	C32735E3 A54942EE F9B35F6C 52145F6B 183CD15D D63C06EA 128ECF9C 5893C3ED
Каталог Release-DLL-x64-skylake	
libCCPPLib-linux.so	7851D492 57AB1406 15FDD88E 2DD776FD EFCC6593 49E896BF D0BDE256 4E99CA49
Каталог Release-DLL-x64-tigerlake	
libCCPPLib-linux.so	C32735E3 A54942EE F9B35F6C 52145F6B 183CD15D D63C06EA 128ECF9C 5893C3ED
Каталог Release-DLL-x64	
libCCPPLib-linux.so	6E1E66E3 317F1D61 A230F475 F344645D FF6B178D 58C4BE8C E5F133C1 5816EE63
Каталог Release-x64-cannonlake	
libCCPPLib-linux.a	168A3AF8 2B4270F1 4B8B07C7 B43F388A F8280188 EDA99E49 D5DE5FDD BF7F76B7
Каталог Release-x64-cascadelake	
libCCPPLib-linux.a	B4F4F93D 94E95613 3B56071C 3A3827ED F725F7A9 4F1F13B3 D9C94982 964BEC34
Каталог Release-x64-cooperlake	
libCCPPLib-linux.a	B4F4F93D 94E95613 3B56071C 3A3827ED F725F7A9 4F1F13B3 D9C94982 964BEC34
Каталог Release-x64-generic	
libCCPPLib-linux.a	901AD72B B0D22914 AC21AE0E 0FE1200D EE4D22AB 4909D496 8A51BD6B 4D619B16
Каталог Release-x64-icelake-client	
libCCPPLib-linux.a	B4F4F93D 94E95613 3B56071C 3A3827ED F725F7A9 4F1F13B3 D9C94982 964BEC34
Каталог Release-x64-icelake-server	
libCCPPLib-linux.a	B4F4F93D 94E95613 3B56071C 3A3827ED F725F7A9 4F1F13B3 D9C94982 964BEC34
Каталог Release-x64-skylake-avx512	
libCCPPLib-linux.a	B4F4F93D 94E95613 3B56071C 3A3827ED F725F7A9 4F1F13B3 D9C94982 964BEC34
Каталог Release-x64-skylake	
libCCPPLib-linux.a	168A3AF8 2B4270F1 4B8B07C7 B43F388A F8280188 EDA99E49 D5DE5FDD BF7F76B7
Каталог Release-x64-tigerlake	
libCCPPLib-linux.a	B4F4F93D 94E95613 3B56071C 3A3827ED F725F7A9 4F1F13B3 D9C94982 964BEC34
Каталог Release-x64	
libCCPPLib-linux.a	758B4719 F9702D62 1B97FDE7 687C5088 CBD6DB51 6E6CD54F FD6D0629 E596F6DC
Каталог x86	
Каталог Release-DLL-x86-generic	
libCCPPLib-linux.so	48228BB8 DB7FAB1A CE373FB6 BDEC1598 C588B54C CBA22881 2421D6C1 FF907984
Каталог Release-DLL-x86	
libCCPPLib-linux.so	A76B7646 6AE293F5 C2AA3DFE 30857943 78F3D27E F093A4BA 07046DD4 53E496DE
Каталог Release-x86-generic	
libCCPPLib-linux.a	595B8D37 C730DFEC 164C1D06 261A3F57 F82BB409 B7245BFD FC87EA91 2C8F981B
Каталог Release-x86	
libCCPPLib-linux.a	CDA97634 617C884D BD660C8D D566A11D AC5DB77E 68BF3F56 BCED0DB0 89703EB8
Каталог ARMv7-32	
Каталог Release-ARMv7-32-cortex-a15.a7	
libCCPPLib-linux.a	70EEA83B 0646C581 3E536B2D 070C858A E8AACA97 D70AA6B6 1BF6D497 C43DE192

Каталог Release-ARMv7-32-cortex-a17
libCCPPLib-linux.a C80150A4 B78C3BE4 038539E1 EFBAFCA3 30B495D0 DD632E85 901CE14F 11187E48
Каталог Release-ARMv7-32-generic
libCCPPLib-linux.a AC3F574E 0F36D7BA 1772B928 2C3491AD BFCF3F60 3EFCED95 1FBE5C0E 1749116D
Каталог Release-ARMv7-32
libCCPPLib-linux.a DAC90EBC 532F608A 384D5D2B 2DBE2964 4638CD89 5DC66D5D D7EE6860 13949D6C
Каталог Release-DLL-ARMv7-32-cortex-a15.a7
libCCPPLib-linux.so 00138114 4FC7D08F CA47C5A4 4103EA62 7CF99886 7659CE9C 4B35C917 30C16342
Каталог Release-DLL-ARMv7-32-cortex-a17
libCCPPLib-linux.so 500B197F E0F61245 BCC082DA D2836D8C C44E9079 23159F43 445EEB23 5ED06302
Каталог Release-DLL-ARMv7-32-generic
libCCPPLib-linux.so F27A243C 711F3C78 D6F9734B A8306B4C 7D0C68DE DA6D1DAB D384C1DD 42D03C7C
Каталог Release-DLL-ARMv7-32
libCCPPLib-linux.so 9100069F 04EB3F5F B74CD7C5 22DE5660 73D1FB74 21989E4E FD0D4234 E50130AC

Каталог ARMv8-64
Каталог Release-ARMv8-64-cortex-a53
libCCPPLib-linux.a 3AAEE667 AFEBC0E8 F3460A79 70F30D7E A0E68578 BB596D74 C7EA041B FA0DEFC0
Каталог Release-ARMv8-64-cortex-a57
libCCPPLib-linux.a 4570A718 311A341E FF4CDB40 A11FA0D5 22541ABE 159A7398 55CDFF7D D6A1B4F6
Каталог Release-ARMv8-64-cortex-a72.a53
libCCPPLib-linux.a 8DA5BCD4 80384117 4414963A 8EDA48A8 6ACA0BFA 65995F54 312A034D 79ACC6FD
Каталог Release-ARMv8-64-generic
libCCPPLib-linux.a 6307F170 136E966C A9C297DD 66522ABD 3A696895 B572B84F 5CE4AFA5 D2492F21
Каталог Release-DLL-ARMv8-64-cortex-a53
libCCPPLib-linux.so 82A2520E CE6C6925 E3B74314 1BCE2A44 28BBF238 9E1B8601 45753746 836C81CA
Каталог Release-DLL-ARMv8-64-cortex-a57
libCCPPLib-linux.so 20788055 7C0C51E0 AC5223FB 53D33FA8 15BB403E C9AB5587 559C9FEB 6E9B9DB9
Каталог Release-DLL-ARMv8-64-cortex-a72.a53
libCCPPLib-linux.so 88312F4A CF5EB74F C6487A18 23D7A331 9E8B6ACB 775374AC A0502AD7 985A66C7
Каталог Release-DLL-ARMv8-64-generic
libCCPPLib-linux.so D7B8EE7D 6CC4CCEB EE94852B 125D4F6A FC1A0F23 810D4E3A A42876F3 898B9DE9

Каталог webassembly
Каталог wasm32
Каталог Release-DLL-wasm-32
libCCPPLib-webassembly.so F28CC1C3 43A8ED34 3A02B1C4 D3C1EB83 7566049B F829871E 647F0D66 78245FF1
Каталог Release-wasm-32
libCCPPLib-webassembly.a B40FBF1E 26ED3E37 CB51BDF3 6D5CA1DC B16EB441 98EB1510 2B9D58EF E1CAF34D

Каталог wasm64
Каталог Release-DLL-wasm-64
libCCPPLib-webassembly.so F28CC1C3 43A8ED34 3A02B1C4 D3C1EB83 7566049B F829871E 647F0D66 78245FF1

Каталог Release-wasm-64
libCCPPLib-webassembly.a B40FBF1E 26ED3E37 CB51BDF3 6D5CA1DC B16EB441 98EB1510 2B9D58EF E1CAF34D

Каталог macOS
Каталог ARM64
libCCPPLib-macOS-dynamic-arm64.dylib 713331E7 980C21D8 67D6771C F59920E8 D4564915 A914C61D A104154B 40A09FAD
libCCPPLib-macOS-static-arm64.a 86BC0DE7 13F60026 459BC313 E9D5B49E E58D5D20 8C2552C6 77641E4F C64DBD4B

Каталог x86-64
libCCPPLib-macOS-dynamic-x86-64.dylib 66D9E513 4A83DB66 AB73A826 88CFC9CF D406D0FF B6129DD1 E82EDD5A 2AA796F2
libCCPPLib-macOS-static-x86-64.a 5D7124B0 8731F2B4 CA5425C9 0F100808 D2B37C1E 521478A6 E5799461 91102FE8

Каталог windows
Каталог x64
Каталог Release DLL-generic
CCPPLib.dll 4F17E45D 0F0800A5 29F63F31 F94AFF6B BEA7A0F4 458F5672 B8BC9EBB 6CA0A2CC
CCPPLib.lib D5174648 3F815FE5 E12E776A CCD2BBD6 51B6B1C4 45DDD545 363C8DC8 B992F851
Каталог Release DLL
CCPPLib.dll 93BA167E CD0E406F E421956D 52A7BB2A 6F67903C 3874F89E 7C802A92 1EC26BC6
CCPPLib.lib D5174648 3F815FE5 E12E776A CCD2BBD6 51B6B1C4 45DDD545 363C8DC8 B992F851
Каталог Release-generic
CCPPLib.lib 5DCADB84 0677DBF4 B65062B5 324268D9 CCBAA807 69ED5221 E4F5FAFE C1C654C9
Каталог Release
CCPPLib.lib 8FBB918F A6252B92 15A1E077 739116D4 403F8E3D 02012344 B69FE561 0ABC4D6B

Каталог x86
Каталог Release DLL-generic
CCPPLib.dll 9AD047DF 2AAEB8CA E8D2D512 BBDDBEE6 982063AB 3A125B94 2BDE66A4 40CDB9E6
CCPPLib.lib 544A47D5 77758007 9F9D0B47 24CD6A01 CCFC1A40 4F1FEDDB EA91F875 513A34DF
Каталог Release DLL
CCPPLib.dll 438C9437 0981E889 13E12A49 82C793B4 7692966F 6BD16B97 1919118F 5AA3573D
CCPPLib.lib 544A47D5 77758007 9F9D0B47 24CD6A01 CCFC1A40 4F1FEDDB EA91F875 513A34DF
Каталог Release-generic
CCPPLib.lib 8FC14100 98212A3E 2CEE7351 9072A59F 937CD908 5A6B6E47 58F312BD 12BE7A0C
Каталог Release
CCPPLib.lib 30434274 9627A274 875055BE D28E2283 65AD1617 EA638DB2 868DD7CF 2020C9A2

Каталог headers
AlgId.h BD1BB0B4 281D0949 C505EC01 00D81D1D 7EB34C7E 68ADE8F7 9EF0B495 8F050D04
ApiDecl.h 0A2D58AD 8B5A9A31 941FB6B1 AE86EAF8 EBF8B9E9 897C9661 6BE21F90 EF62BCF1
CCPPLib.h DD1A5A77 5E5409B4 21473115 EAA65860 D181B197 16D8B655 F32428C5 F21C6DFB
CryptoErrors.h D894DC25 BBD730D0 38BA17F5 7DFB916F 8ADEEE47 CB038584 54867B31 BEA4CEAC
DSTU4145Params.h 30FC8713 C533339C 5A6D4AEB CB96A6F9 74C0EC10 CAA4F4F5 D394AC05 E683C423
DSTU7624Params.h 30716AA7 CD83A857 6CA3A40C 1E54FE0B 0F8B6F79 21039D18 F51EC122 6FF94FB9
DSTU9041Params.h EC3B25E9 D2A03F13 0BCAFCB4 FDFA5212 02FDE93D 9FB7C74A 689E60DE B6CB80FD
FIPS1863Params.h 65D71F64 74ACECA6 7BC4B1E0 BE85C77C 38DEF631 F1ECA284 9B826815 712139C9
GOST28147Params.h 91AE6ADD 310A2C37 CE73D039 7BAC6D9F 520DE690 759A6F27 86570155 4668BF07

IBigNum.h	F0D80046 09D71F84 3A8F7EB7 60A4D174 C972D7F2 01709AC7 9DB54370 4725E23B
ICommonSystemParams.h	7877D28D 4C4E93DB C9B26520 405D65E4 121608BB 3514747C BF840611 50CAB4BE
IECPoint.h	158BEAA6 25FC2A5B 6C038FB4 AC523C12 54AAD4BA F415A051 E5B34FB1 CEE30D19
IHash.h	4476AE7D 8CD65F88 A9A6CC7A 6D41D8B4 F267C03A C3FF9775 52121251 4AF5F266
IKDF.h	02BACFCE 22FB5E20 2D4148A1 B79A395D E0A9B4EB 16ABDE93 35B535E1 D4EAB9E4
IKeyedDigest.h	52E75474 83FC904B C3794A47 242BF391 A0FE4DD2 FC9DE02E 8359B051 52F962B4
IMEM.h	C18EBCA5 E3BFAA6E 4DF326D2 01091AF1 0DA534C5 DD980049 EF6A33F8 83B7964B
IMsgDigest.h	3F8C6447 68D19916 1D7DA683 F6158890 0D25D604 EBF1DC89 227BE69C 686DC8F2
InnerMacros.h	8B7DDB0A B68CBA3E D621C7BF E1A0876C 2664645C 4F09F639 5145ED42 DA891928
IPBES.h	C1A33795 D47F3005 C1FEAF13 78955CFB EBB6456A 203A79FD BE8DBD9A DE3FA26F
IPBKeyedDigest.h	1C9F9A49 58D4D3C8 289D6CE1 21A993B5 4DEE601E 5ACFB831 162CBACF F265EE27
IPrivateKey.h	68C35328 B3812B87 9D349096 E093AEB5 ABB03D01 4698D019 2725C198 6549B8BD
IPublicKey.h	C790D00D 6F38150E 9B7B4FF7 489C2FE2 B8A5E732 16B1512D 3936B259 58403446
IRNG.h	3B19A39E 8F6F436B DC2A585F B2AB92BA 8D84B2E8 1A1AD70B 06F04F1D 681B98EE
ISignature.h	85602E03 2FC1BA73 F7CDBBBF 0A14550F 81EC12ED 2078ECB2 F4E1FD0E 2E791829
ISymCipher.h	4765ECA5 00C7C0A8 011132C2 CDC090F4 1A35EA17 DDFFE1D1 4FE54894 4AE6DEC2
RFC5639Params.h	EAF2B2E6 E6CEBBD2 F2E54A50 E033B699 4F243191 A410F920 0BFDD69C 11EC0849
RFC8032Params.h	D2787D34 49BF338F 2CC86A0C E4C56905 C1720C44 5CCF0192 C2757D55 AFC68716
SystemParams.h	F619AB46 9BFE3A0E 8A25D40C 5F4C7088 984BCDCF D8A624BE B1490AD5 EB71A894
UAGovParams.h	42C3DB14 CF3AFB5F B9B25A7B 0C0A205E 72E3AFDD 9ECCD992 4682213E 138CCD98

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 18.08.2027.

Голова Служби Юрій ЩИГОЛЬ