



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@dssz.gov.ua

19.12.17 № 04-3416

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 19.12.2017

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 19.12.2017 № 327.

Об'єкт експертизи: Комплекс програмний центру сертифікації ключів «ІТ ЦСК-1»
(версія 1.3) ТУ У 62.0-22723472-028:2016.

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, ГОСТ 34.311-95, ДСТУ 4145-2002 (в поліноміальному базисі з довжиною ключа 163 – 509 біт).
2. В об'єкті експертизи правильно реалізовано криптографічні алгоритми шифрування TDEA і AES відповідно до ДСТУ ISO/IEC 18033-3:2015 (в режимі CBC, визначеному ДСТУ ISO/IEC 10116:2014).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису RSA, визначений PKCS#1 v2.1: RSA Cryptography Standard (за схемою RSASSA-PKCS1-v1_5).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2014.
5. В об'єкті експертизи правильно реалізовано криптографічні алгоритми генування SHA-1, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм генування SHA-224, визначений FIPS PUB 180-4.
7. В об'єкті експертизи правильно реалізовано протокол розподілу ключів RSA (алгоритм направлено шифрування), визначений PKCS#1 v2.1: RSA Cryptography Standard (за схемою RSAES-PKCS1-v1_5).
8. 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.

9. В об'єкті експертизи алгоритм генерації ключових даних відповідає документу «Методика генерації ключових даних ЄААД.468244.020 Д1.05».

10. Об'єкт експертизи відповідає вимогам технічного завдання ЄААД.468244.021 ТЗ із доповненнями № 1, № 2, № 3, № 4 до нього в частині реалізації функцій криптографічних перетворень.

11. 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, які реалізовані та/або 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 в Міністерстві юстиції України 20.08.2012 за № 1398/21710.

12. Формати криптографічних повідомлень та протоколи розподілу ключів, які реалізовані та/або використовуються 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 в Міністерстві юстиції України 14.01.2013 за № 108/22640.

13. Алгоритми формування ключів шифрування ключів та захисту особистих ключів електронного цифрового підпису та особистих ключів шифрування, формати транспортних контейнерів особистих ключів електронного цифрового підпису та особистих ключів шифрування, контейнерів зберігання особистих ключів електронного цифрового підпису, особистих ключів шифрування та сертифікатів відкритих ключів, які реалізовані та/або використовуються в об'єкті експертизи, 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.

14. В об'єкті експертизи правильно реалізовано вимоги IETF RFC 2560, IETF RFC 3161, IETF RFC 5652, PKCS #7, PKCS #8, PKCS #10, PKCS #12, ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3, ETSI EN 319 412-5 у частині їх використання в національній інфраструктурі відкритих ключів.

15. 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.

16. Об'єкт експертизи може бути застосований для побудови акредитованого центру сертифікації ключів, у тому числі центрального засвідчувального органу.

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи, виготовлені відповідно до технічних умов ТУ У 62.0-22723472-028:2016 зі Зміною № 1 до них.

Термін дії експертного висновку – до 19.12.2022.

Перший заступник Голови Служби



О.М. Чаузов



ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03680,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszz.gov.ua

05.04.2016 № 05/од/08-1484

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: *05.04.2016*

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 31.03.2016 № 234.

Об'єкт експертизи: Комплекс програмний користувача центру сертифікації ключів
"ІТ Користувач ЦСК-1" ЄААД.00021-13 90 02.

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 реалізовані криптографічні алгоритми, які визначені ДСТУ ГОСТ 28147:2009, ГОСТ 34.311-95, ДСТУ 4145-2002.
2. В об'єкті експертизи правильно реалізовано криптографічні алгоритми шифрування TDEA і AES відповідно до ДСТУ ISO/IEC 18033-3:2015 (в режимі CBC, що визначений ДСТУ ISO/IEC 10116:2014).
3. В об'єкті експертизи правильно реалізовано криптографічні алгоритми ґешування SHA-1, SHA-256, SHA-384, SHA-512, які визначені в ДСТУ ISO/IEC 10118-3:2005.
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм ґешування SHA-224, який визначений в FIPS PUB 180-4.
5. В об'єкті експертизи правильно реалізовано криптографічний протокол автономного узгодження ключів типу Діффі-Гелмана (KANIDH), який наведено в п. 8.2 ДСТУ ISO/IEC 15946-3:2006.
6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений PKCS#1 v.2.1 "RSA Cryptography Standard (за схемою RSAES-PKCS1-v1_5), IETF RFC 3447.
7. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису RSA, визначений PKCS#1 v.2.1 "RSA Cryptography Standard (за схемою RSASSA-PKCS1-v1_5), IETF RFC 3447.
8. В об'єкті експертизи алгоритм генерації ключових даних відповідає документу "Методика генерації ключових даних ЄААД.468244.020 Д1.05".

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, які реалізовані та 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 від 20.08.2012 за № 1398/21710.

10. Формати криптографічних повідомлень, які реалізовані та використовуються 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. Формат та вміст файлів сховищ особистих ключів електронного цифрового підпису, які реалізовані в об'єкті експертизи, відповідають вимогам спільного 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. В об'єкті експертизи правильно реалізовано вимоги IETF RFC 2560, IETF RFC 3161, IETF RFC 5652, PKCS #7, PKCS #8, PKCS #12 у частині їх використання в національній інфраструктурі відкритих ключів.

13. Об'єкт експертизи відповідає вимогам технічного завдання ЄААД.00021-13 90 02-1 із Доповненням № 1 ЄААД.00021-13 90 02-2 та Доповненням № 2 ЄААД.00021-13 90 02-3 до нього, в частині реалізації функцій криптографічних перетворень.

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): для експертного висновку поширюється на зразки об'єкта експертизи, які виготовлені відповідно до технічних умов ТУ 72.2-22723472-008:2011 зі Змінами № 1, № 2, № 3 до них.

Термін дії експертного висновку – до 31.03.2021.

Перший заступник Голови Служби



О.М. Чаузов



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

26.12.17 № 04-3507

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: __.12.2017 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 22.12.2017 № 328.

Об'єкт експертизи: КРИПТОМОДУЛЬ МЕРЕЖНИЙ «ГРЯДА-301» СААД.469535.049,
СААД.469535.240, СААД.469535.241, СААД.469535.243.

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 ДСТУ ГОСТ 28147:2009 (в режимах простої заміни, гамування зі зворотнім зв'язком та вироблення імітовставки), ГОСТ 34.311-95, ДСТУ 4145-2002.
2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений PKCS#1 v2.2 RSA Cryptography Standard (за схемою RSAES-PKCS1_v1_5).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2014.
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису RSA, визначений PKCS#1 v2.2: RSA Cryptography Standard (за схемою RSASSA-PKCS1-v1_5).
5. 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.
6. В об'єкті експертизи забезпечується захист записаних даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.
7. Формати криптографічних повідомлень та протоколи розподілу ключів, що реалізовані та/або використовуються 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 в Міністерстві юстиції України 14.01.2013 за № 108/22640.

2

8. Об'єкт експертизи відповідає вимогам технічного завдання СААД.469535.049 ТЗ із Доповненнями № 1, № 2, № 3, № 4, № 5, № 6 в частині реалізації функцій криптографічних перетворень.

9. 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 26.2-22723472-003:2017.

Термін дії експертного висновку – до 22.12.2022.

Перший заступник Голови Служби



О.М. Чаузов