



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

13.07.2018 № 04/03/02 - 2954

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 13.07.2018

м. Київ

Виданий: Товариству з обмеженою відповідальністю «Техноконсалтинг»
(код ЄДРПОУ 25284317)

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 19.07.2018 № 354.

Об'єкт експертизи: Засіб електронного цифрового підпису апаратно-програмний «Tellipse3»
25284317.467649.003.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю
«Техноконсалтинг» (код ЄДРПОУ 25284317).

Експертний заклад: Інститут спеціального зв'язку та захисту інформації НТУУ
«КПІ імені Ігоря Сікорського» (код ЄДРПОУ 34979237).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування електронного цифрового підпису, визначений ДСТУ 4145-2002 (у поліноміальному базисі).
2. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений IETF RFC 3447 (за схемою RSAES-PKCS1-v1_5).
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного цифрового підпису RSA, визначений IETF RFC 3447 (за схемою RSASSA-PKCS1-v1_5).
4. В об'єкті експертизи забезпечується захист записаних даних від несанкціонованого доступу від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.
5. Об'єкт експертизи відповідає вимогам технічного завдання на дослідно-конструкторську роботу Розробка надійного засобу електронного цифрового підпису на базі мікропроцесорної картки, шифр «Tellipse3», із Доповненням № 1 до нього, в частині реалізації функцій криптографічних перетворень.
6. 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 26.1-25284317-003:2013 зі зміною № 1 до них.

Термін дії експертного висновку – до 19.07.2023.

Голова Служби



Л.О. Євдоченко