Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

01034, м. Київ, вул. Паторжинського, 5/7,
тел. (044) 281-90-10, факс: (044) 226-26-83, e-mail: info@dsszzi.gov.ua

07.06.2012 № 05/02/02-2474

ЕКСПЕРТНИЙ ВИСНОВОК

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 07.06.2012 № 89.

Об'єкт експертизи: Засіб електронного цифрового підпису апаратно-програмний "TEllipseST".

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

Експертний заклад: Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ" (код ЄДРПОУ 34979237).

Висновки:
1. В об'єкті експертизи алгоритм формування електронного цифрового підпису відповідає вимогам ДСТУ 4145-2002 (у поліноміальному базисі).
2. В об'єкті експертизи алгоритм формування електронного цифрового підпису відповідає вимогам алгоритму RSA, який визначений IETF RFC 3447 (схема RSASSA-PKCS1-v1_5).
3. В об'єкті експертизи алгоритм асиметричного шифрування відповідає вимогам алгоритму RSA, який визначений IETF RFC 3447 (схема RSAES-PKCS1-v1_5).
4. Об'єкт експертизи відповідає технічному завданню "Розробка надійного засобу електронного засобу цифрового підпису" шифр "TEllipseST" та технічним умовам "Засіб електронного цифрового підпису апаратно-програмний "TEllipseST" (ТУ У 30.0-25284317-002:2011) в частині реалізації функцій криптографічних перетворень.

Особливі умови (рекомендації): Дія експертного висновку поширюється на зразки об'єкта експертизи, які виготовлені відповідно до технічних умов ТУ У 30.0-25284317-002:2011.

Термін дії експертного висновку: до 07.06.2017.

Перший заступник Голови Служби О. Г. Цуркан

Адміністрація Державної служби спеціального зв'язку та захисту інформації України
Ідентифікаційний код 34620942