Прим. № 1

# 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@dsszzi.gov.ua

29.08.2013 № 05/02/02-3091

## ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 29.08.2013 м. Київ

Виданий: Товариству з обмеженою відповідальністю "Інформейшн Сістемс Сек'юріті Партнерс" (код ЄДРПОУ 36351406)

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 29.08.2013 № 124.

Об'єкт експертизи: Апаратно-програмні вироби криптографічного захисту інформації Gemalto IDPrime .Net (IDPrime .Net 510, IDPrime .Net 511, IDPrime .Net 7519 USB Token, IDPrime .Net 7510, IDPrime .Net 5500, IDPrime .Net 5501).

Розроблений (виготовлений): Компанією "Gemalto NV", Нідерланди.

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

Висновки:
1. В об'єктах експертизи алгоритми шифрування та електронного цифрового підпису відповідають алгоритму RSA, визначеному в IETF RFC 3447.
2. В об'єктах експертизи алгоритм гешування відповідає алгоритму MD5, визначеному в IETF RFC 1321.
3. В об'єктах експертизи алгоритм гешування відповідає алгоритму SHA-1, визначеному в розділі 9 ДСТУ ISO/IEC 10118-3:2005.
4. В об'єктах експертизи алгоритм гешування відповідає алгоритму SHA-256, визначеному в розділі 10 ДСТУ ISO/IEC 10118-3:2005.
5. В об'єктах експертизи алгоритм гешування відповідає алгоритму HMAC-SHA-1, визначеному в FIPS PUB 197.

Особливі умови (рекомендації): Дія експертного висновку поширюється на зразки об'єктів експертизи із заводськими номерами:
- Виріб IDPrime .Net 510: 5701135122628A182513FFFF, 5701135122628A182613FFFF, 5701135122628A182313FFFF;
- Виріб IDPrime .Net 511: 57011351225B12133A15FFFF, 57011351225B12133715FFFF, 57011351225B12133915FFFF;
- Виріб IDPrime .Net 7519 USB Token: NET00000652A, NET00000652B, NET00000611E;
- Виріб IDPrime .Net 7510: GANC00005020, GANC00005021, GANC00005024;
- Виріб IDPrime .Net 5500: 57011351223454080E21FFFF, 57011351223454080A21FFFF, 57011351223454080D21FFFF;
- Виріб IDPrime .Net 5501: 57011351225B12133615FFFF, 57011351225B12133315FFFF, 57011351225B12130816FFFF.

Термін дії експертного висновку – до 29.08.2016.

Перший заступник Голови Служби О.Г. Цуркан