Апаратно-програмний засіб криптографічного захисту інформації – носій ключової інформації "Ефіт Key"

Виробник: Товариство з обмеженою відповідальністю "Ефіт технолоджіс"

Експертний висновок Державної служби спеціального зв'язку та захисту інформації України від 12.10.2015 № 05/02/02-4326

Апаратно-програмний засіб криптографічного захисту інформації – носій ключової інформації "Ефіт Key" (далі - Електронний ключ) - призначений для використання в інформаційних та інформаційно-телекомунікаційних системах, системах електронного документообігу, електронного банкінгу, електронного трейдингу, державних електронних реєстрах, електронних платіжних системах з метою забезпечення авторизації користувачів, а також забезпечення захищеного формування, використання та зберігання особистих ключів електронного цифрового підпису та шифрування (узгодження ключів).

Електронний ключ виконаний у вигляді малогабаритного знімного USB-пристрою, який має міцний пластиковий корпус.

Електронний ключ реалізує наступні криптографічні алгоритми та протоколи:

- шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни та режим вироблення імітовставки);
- шифрування за RSA (довжини ключів довжина ключа – 512-2048 біт);
- ЕЦП за ДСТУ 4145-2002 (довжини ключів передбачені стандартом);
- ЕЦП за RSA (довжини ключів довжина ключа – 512-2048 біт);
- гешування за ГОСТ 34.311-95;
- гешування за SHA;
- гешування за SHA-256.
- протокол розподілу ключових даних Діффі-Гелмана в групі точок еліптичної кривої;

Швидкість формування ЕЦП за ДСТУ 4145-2002, поле 257 - 100 мс.

Швидкість формування ЕЦП за RSA, поле 1536 - 400 мс.

ЕФІТ ТЕХНОЛОДЖІС

Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливлює доступ до особистих ключів з боку апаратного-програмного середовища.

Особисті ключі генеруються, зберігаються та використовуються тільки усередині електронного ключа, та жодним способом не потрапляють за його межі. Зберігання особистих ключів та інших ключових даних здійснюється у внутрішньому постійному запам’ятовуючому пристрої електронного ключа.

Виготовляється на базі мікроконтроллера ST32F2xx (ARM архітектура центрального процесора).

Об'єм пам'яті: 256 Кбайт.

Інтерфейси і стандарти, що підтримуються:

- MS Smart Card Minidriver;
- MS CCID Smart Cards;
- PC/SC Smart Card;
- PKCS#11;
- MS Smart Card Base CSP;
- USB v1.0, USB v2.0.

Електронний ключ підтримує роботу з наступними операційними системами:

- Microsoft Windows (x86, x64) починаючи від XP по 10 (включно);
- Linux (x86, x64).

Захист від підбору паролю: вбудована технологія, що дозволяє здійснити захист паролю користувача електронного ключа від атаки "повного перебору", що в свою чергу дозволяє захистити особисті ключі електронного цифрового підпису та шифрування (узгодження ключів) власника електронного ключа від їх несанкціонованого використання.

Термін експлуатації - 15000 годин протягом 10 років.

Гарантія – 36 міс.

Електронний ключ підтримується у наступних продуктах:

- спеціалізоване програмне забезпечення робочих станцій видачі та перевірки біометричних паспортів громадян України для виїзду за кордон та паспортів громадян України у формі ID-картки;
- Microsoft Office Word;
- Microsoft Office Outlook;
- Mozilla Thunderbird;
- TheBat!;
- Mozilla Firefox;
- Internet Explorer;
- Adobe Acrobat;
- Open VPN;
- OpenSSL;
- GnuPG/OpenPGP;
- TrueCrypt;
- SeaMonkey;
- BitLocker Drive Encryption;
- CryptoAutograph;
- iGov.org.ua.