ООО «АВТОР»
ул. Смоленская, 31-33, Киев, 03005,
Украина т/ф +380 44 538 00 89

НОСИТЕЛИ КЛЮЧЕВОЙ ИНФОРМАЦИИ

Носители ключевой информации (НКИ) компании «АВТОР» – это универсальный инструмент, предназначенный для использования в инфраструктуре открытых ключей (PKI), платежных системах, системах доступа, сетевой безопасности, в качестве электронного идентификатора, носителя персональной информации, а также средства формирования ЭЦП с неизвлекаемым закрытым ключом.

Смарт-карта «CryptoCard-337» с использованием USB карт-ридера

Электронный ключ «SecureToken-337»

Миниатюрный электронный ключ «SecureToken-337 mini»

Электронный ключ «SecureToken-337F»

Начиная с 2013 года копания «АВТОР» выпускает НКИ в миниатюрном корпусе – «SecureToken-337 mini» , а также НКИ с Flash-памятью – «SecureToken-337F».

Назначение НКИ

Основное назначение НКИ заключается в защищенном хранении и использовании ключевой информации, обеспечении целостности, аутентичности и сокрытия содержания данных, которые обрабатываются от навязывания неправдивой информации, а также защиты от несанкционированного доступа благодаря применению средств электронной цифровой подписи, шифрования и аутентификации.

Благодаря применению надежных аппаратных, технологических и программных методов защиты от несанкционированного доступа к сохраненной в НКИ информации, отсутствует необходимость создания сложного ПИН-кода доступа к нему. **Использование ПИН-кодов с длиной от 4 до 8 символов упростит и ускорит работу с НКИ, при сохранении высокого уровня защиты от несанкционированного доступа.**

Основные возможности НКИ:

- генерация ключевых данных и формирование ЭЦП в соответствии с ДСТУ 4145-2002 с длиной ключа – 163-509 бит;
- шифрование/расшифровывание данных (ГОСТ 28147-89);
- вычисление хеш-функции (ГОСТ 34.311-95);
- генерация личных ключевых данных и формирование ЭЦП в соответствии с PKCS#1 RSA Cryptography Standard, с длиной ключа 512-2048 бит;
- расшифрование сообщений в соответствии с PKCS#1 RSA Cryptography Standard, с длиной ключа 512-2048 бит;
- хранение на НКИ до 30 личных ключей;
- хранение информации пользователя на электронных ключах «SecureToken-337» с Flash-памятью (доступны модификации с объемом памяти от 2 Гб до 32 Гб).

Основные технические характеристики

	CryptoCard-337 **SecureToken-337**	**Комментарии**
Общие сведения		
Форм-фактор	• USB-ключ • Миниатюрный USB-ключ • Смарт-карта	Основные функциональные возможности USB-ключа и смарт-карты не отличаются, так как они построены на базе одного смарт-чипа компании NXP Semiconductors P5CC037
Размер Flash-памяти	От 2 Гб до 32 Гб	Только для «SecureToken-337F»

Архитектура		
Аппаратная		
Смарт-чип	Смарт-чип компании NXP Semiconductors P5CC037	Смарт-чип имеет несколько уровней защиты от несанкционированного доступа к сохраненной в нем информации: аппаратный, технологический и программный. Смарт-чипы обладают встроенной защищенной памятью, средствами противодействия различным атакам. Надежность данных смарт-чипов подтверждается сертификацией по уровню Common Criteria EAL5+
RAM	6КБ	
ROM	200КБ	
EEPROM	36КБ	
USB	USB2.0 Full-speed	«SecureToken-337», «SecureToken-337 mini»
	USB2.0 Hi-speed	«SecureToken-337F»
Программная		
ОС	«УкрКОС 3.0»	Гарантированный уровень безопасности ОС «УкрКОС 3.0» обеспечивается благодаря разделению ядра системы и разных приложений, которые в свою очередь работают независимо друг от друга, имея персональные механизмы защиты. Все операции выполняются в защищенной памяти смарт-чипа. Компания «АВТОР» гарантирует, что у ОС «УкрКОС 3.0» не существует команды, которая позволяет извлечь секретный ключ из памяти смарт-чипа. Сегодня в Украине в разных проектах (ЭЦП, двухфакторная авторизация, шифрование, платежные и др.) работает более 4 млн. НКИ с ОС «УкрКОС»
Криптографическая подсистема		
Аппаратная реализация украинских криптографических алгоритмов		
ЭЦП	Формирование и проверка ЭЦП согласно ДСТУ 4145-2002	длина ключа – 163-509 бит
Хеширование	Вычисление значения хэш-функции в соответствии с ГОСТ 34.311-95	

Шифрование	Шифрование информации в режимах простой замены, гаммирования с обратной связью, вычисления имитовставки согласно ДСТУ ГОСТ 28147-89	
Аппаратная реализация зарубежных алгоритмов		
Симметричное шифрование	DES / 3DES, AES (128, 192, 256 бит)	
ЭЦП	RSA (512/1024/2048/4096 бит)	
Асимметрич-ное шифро-вание	RSA (512/1024/2048/4096 бит)	
Хеширование	SHA-1, SHA-256	
Возможности встраивания		
Наличие комплекта разработчика	• Комплект документации • Примеры исходных кодов • Библиотека взаимодействия и дополнительное ПО	Комплект для разработки позволяет провести интеграцию НКИ в различные системы клиента.
Доступные интерфейсы и стандарты	• PKCS#11 v2.20 • Microsoft Crypto API (CAPI) • Microsoft Crypto API : Next Generation (CNG) • APDU команды • Java Cryptography Architecture (JCA) • Сохранение сертификатов X.509 v3 • SSL v3, IPSec/IKE • Minidriver • Microsoft CCID	Данные интерфейсы обеспечивает возможность интеграции НКИ с операционными системами, прикладными программными комплексами и Центрами сертификации ключей
Поддержи-ваемые ОС	• MS Windows 7 (32/64-біт) • MS Windows Vista (32/64-біт) • MS Windows XP (32/64-біт) • MS Windows Server 2008 R2 • MS Windows Server 2008 (32/64-біт) • MS Windows Server 2003 R2 (32/64-біт) • MS Windows Server 2003 (32/64-біт) • Mac OS X (PKCS#11, интерфейс APDU-команд) • Linux (PKCS#11, JCA, интерфейс APDU-команд)	• Windows (PKCS#11, Windows CRYPTOAPI, JCA, интерфейс APDU-команд)

Надежность		
Гарантия	12 месяцев	
Время наработки на отказ	Гарантируемое время хранения данных в энергонезависимой памяти – 25 лет. Не менее 500 000 циклов чтения/записи.	
Международные сертификаты совместимости и соответствия	Смарт-чипы NXP P5CC037 сертифицированы на уровень Common Criteria EAL5+	
Удобство эксплуатации		
Работа без установки драйверов	Да, CCID-совместимость	«SecureToken-337», «SecureToken-337 mini », «SecureToken-337F »
Дополнительные возможности (RFID, печать, цвет)	• Встраивание RFID –метки • Печать на смарт-карте • Различные цвета корпуса	ООО «АВТОР» предлагает широкие возможности по выбору стиля своих НКИ.

Скоростные характеристики НКИ

В таблице ниже приведены скоростные характеристики формирования ЭЦП носителями ключевой информации компании «АВТОР» в соответствии с национальными и международными стандартами.

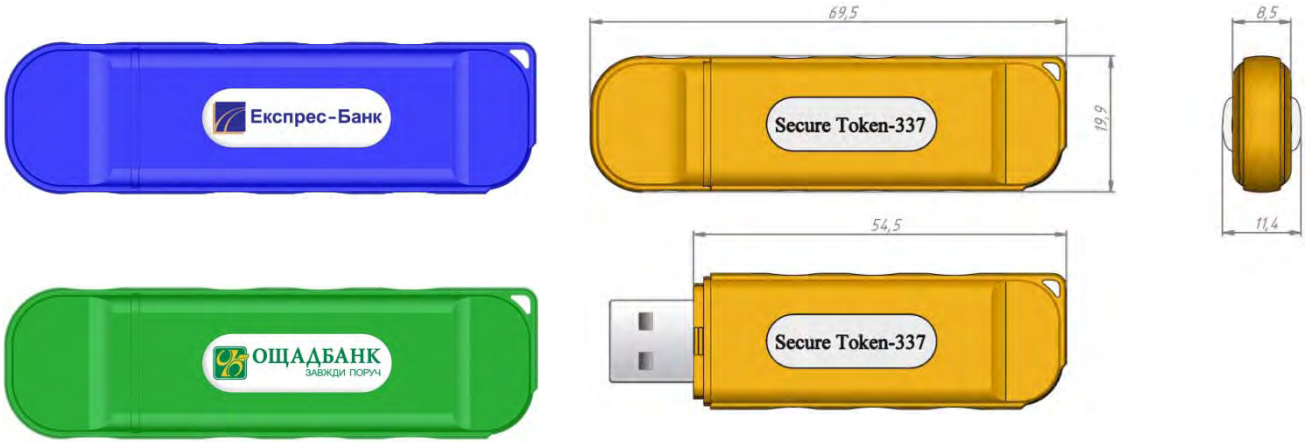
Название стандарта	Длина ключа, бит	Время формирования ЭЦП, мс
ДСТУ 4145-2002	191	30
	257	50
	509	185
PKCS#1 RSA Cryptography Standard	1024	300
	1536	1000
	2048	2000

Преимущества НКИ

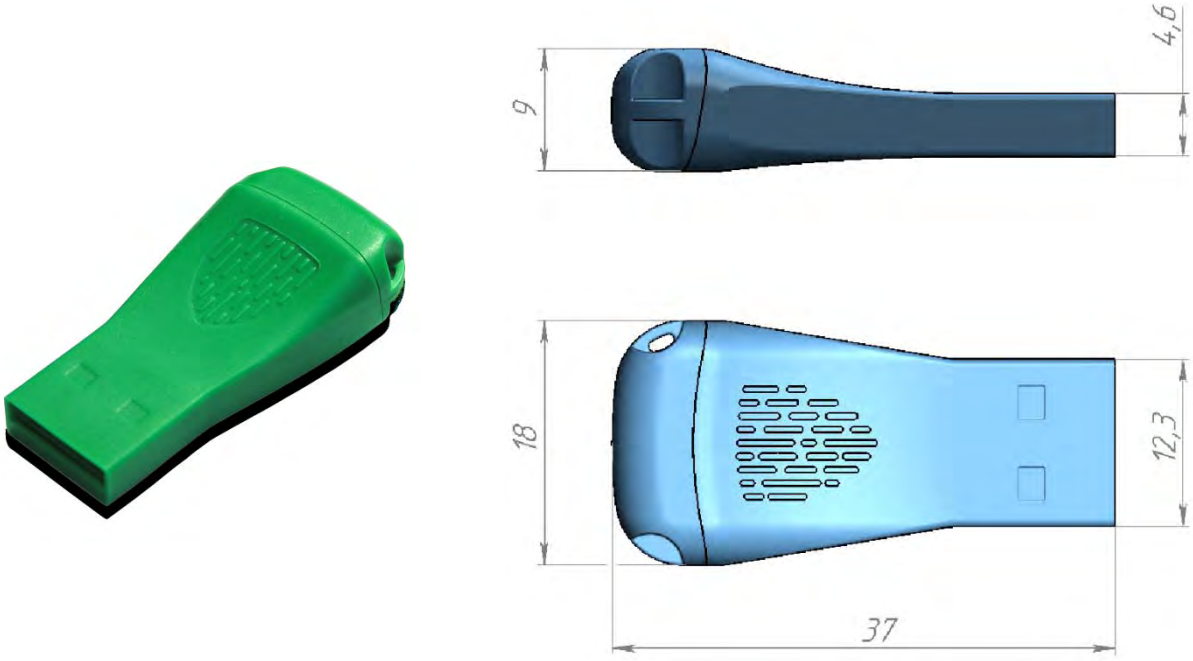
Популярность НКИ в последнее время становится все выше, и это связано с тем, что они имеют высокий уровень защиты по сравнению с обычными дисками или «флешками», а также незащищенными пассивными usb-ключами:

- НКИ имеют надежную встроенную систему защиты от считывания и подмены информации (эта особенность защищает ее владельца от случаев любого нелегального копирования и несанкционированного использования его ключевой информации);
- обмен информацией с НКИ происходит в зашифрованном виде, потому ее просто невозможно перехватить или изменить (эта возможность позволяет со стопроцентной уверенностью утверждать, что информация не будет рассекреченной);
- долговечность (НКИ не склонны к влиянию электромагнитных излучений и менее склонны к влиянию воды, грязи и химикатов);
- соответствие уровню защищенности даже по европейским критериям (смарт-чипы, используемые в НКИ компании «АВТОР», отвечают уровню CC EAL5+);
- возможность хранений от 2 Гб до 32 Гб личной информации пользователя на НКИ как в открытом, так и в зашифрованном виде (устройство «SecureToken-337F»).

Дизайн Электронных ключей «SecureToken-337» и «SecureToken-337F»



Дизайн миниатюрных Электронных ключей «SecureToken-337 mini»



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

11.03.2013 № 05/02/02-209

ЕКСПЕРТНИЙ ВИСНОВОК

Виданий: Товариству з обмеженою відповідальністю "Автор" (код ЄДРПОУ 32248356)

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 11.03.2013 № 108.

Об'єкт експертизи: Електронний ключ "Secure Token-337" (ТУ У 30.0-32248356-017:2011).

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "Автор" (код ЄДРПОУ 32248356).

Експертний заклад: Адміністрація Державної служби спеціального зв'язку та захисту інформації України.

Висновки:

1. В об'єкті експертизи правильно реалізовані криптографічні протоколи та алгоритми, які визначені ДСТУ ГОСТ 28147:2009 (в режимах простої заміни, гамування із зворотнім зв'язком, обчислення імітовставки), ГОСТ 34.311-95 (для нульового стартового вектора), SHA-1 відповідно до ДСТУ ISO/IEC 10118-3:2005, DES, TripleDES, AES у режимах ECB, CBC, CBF, відповідно до ISO/IEC 18033-3:2005 і ISO/IEC 10116-3:2006.
2. Реалізація алгоритму ЕЦП (формування та перевіряння ЕЦП) відповідає ДСТУ 4145-2002 для степенів поля від 163 до 509 бітів у поліноміальному базисі та PKCS#1 v2.1 "RSA Cryptography Standard" за схемою RSASSA-PKCS1-v1.5.
3. Порядок формування та розподілу сеансових ключів алгоритму ДСТУ ГОСТ 28147:2009 відповідає документу "Засоби КЗІ. Методика вироблення сеансового ключа, автентифікації, генерування випадкових послідовностей та контролю засобів КЗІ. АЧСА.460709.001" для степенів поля еліптичної кривої від 163 до 509 бітів у поліноміальному базисі.
4. Порядок формування та розподілу сеансових ключів алгоритму ДСТУ ГОСТ 28147:2009 відповідає алгоритму ECDH для степенів поля еліптичної кривої від 163 до 509 бітів у поліноміальному базисі.
5. Об'єкт експертизи може бути використаний для побудови засобів 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, які виготовлені відповідно до технічних умов (ТУ У 30.0-32248356-017:2011).

Термін дії Експертного висновку: до 22.04.2016.

Перший заступник Голови Служби О.Г. Цуркан

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

11.03.2013 № 05/02/02-810

ЕКСПЕРТНИЙ ВИСНОВОК

Виданий: Товариству з обмеженою відповідальністю "Автор" (код ЄДРПОУ 32248356)

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 07.03.2013 № 108.

Об'єкт експертизи: Мікропроцесорна картка "CryptoCard-337" (ТУ У 30.0-32248356-016:2011).

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "Автор" (код ЄДРПОУ 32248356).

Експертний заклад: Адміністрація Державної служби спеціального зв'язку та захисту інформації України.

Висновки:

1. В об'єкті експертизи правильно реалізовані криптографічні протоколи та алгоритми:, які визначені ДСТУ ГОСТ 28147:2009 (в режимах простої заміни, гамування із зворотнім зв'язком, обчислення імітовставки), ГОСТ 34.311-95 (для нульового стартового вектора), SHA-1 відповідно до ДСТУ ISO/IEC 10118-3:2005, DES, TripleDES, AES у режимах ECB, CBC, CBF, відповідно до ISO/IEC 18033-3:2005 і ISO/IEC 10116-3:2006.
2. Реалізація алгоритму ЕЦП (формування та перевіряння ЕЦП) відповідає ДСТУ 4145-2002 для степенів поля від 163 до 509 бітів у поліноміальному базисі та PKCS#1 v2.1 "RSA Cryptography Standard" за схемою RSASSA-PKCS1-v1.5.
3. Порядок формування та розподілу сеансових ключів алгоритму ДСТУ ГОСТ 28147:2009 відповідає документу "Засоби КЗІ. Методика вироблення сеансового ключа, автентифікації, генерування випадкових послідовностей та контролю засобів КЗІ. АЧСА.460709.001" для степенів поля еліптичної кривої від 163 до 509 бітів у поліноміальному базисі.
4. Порядок формування та розподілу сеансових ключів алгоритму ДСТУ ГОСТ 28147:2009 відповідає алгоритму ECDH для степенів поля еліптичної кривої від 163 до 509 бітів у поліноміальному базисі.
5. Об'єкт експертизи може бути використаний для побудови засобів 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, які виготовлені відповідно до технічних умов (ТУ У 30.0-32248356-016:2011).

Термін дії Експертного висновку: до 22.04.2016.

Перший заступник Голови Служби О.Г. Цуркан

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

11.03.2015 р. № 05/02/02-934

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 11.03.2015 м. Київ

Виданий: Товариству з обмеженою відповідальністю "АВТОР" (код ЄДРПОУ 32248356)

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 11.03.2015 № 184.

Об'єкт експертизи: КЛЮЧІ ЕЛЕКТРОННІ "SECURE TOKEN-337Fx" АЧСА.467369.018.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "АВТОР" (код ЄДРПОУ 32248356).

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 ГОСТ 34.311-95, ДСТУ 4145-2002 (у поліноміальному базисі), ДСТУ ГОСТ 28147:2009 (в режимах простої заміни, гамування із зворотнім зв'язком та виробленням імітовставки).
2. В об'єкті експертизи правильно реалізовані криптографічні алгоритми шифрування DES, TDEA, AES, які визначені в ISO/IEC 18033-3:2010, в режимах ECB, CBC, CFB, які визначені в ISO/IEC 10116:2006.
3. В об'єкті експертизи правильно реалізований криптографічний алгоритм гешування SHA-1, який визначений ДСТУ ISO/IEC 10118-3:2005.
4. В об'єкті експертизи правильно реалізований криптографічний алгоритм шифрування RC5 в режимі CBC, який визначений в IETF RFC 2040.
5. В об'єкті експертизи правильно реалізований криптографічний алгоритм RSA, який визначений PKCS#1 v2.1 "RSA Cryptography Standard" (у варіантах реалізації RSASSA-PKCSl-vl_5 та RSAES-PKCSl-vl_5 з довжиною ключа 1024, 2048 бітів).
6. Формати криптографічних повідомлень та протокол узгодження ключів ECDH, 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 в Міністерстві юстиції України 14.01.2013 за № 108/22640.
7. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ.АЧСА.467369.018-01 та Доповнення № 1 до нього в частині реалізації функцій криптографічних перетворень.
8. 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 (моделі електронного ключа "SECURE TOKEN-337F4", "SECURE TOKEN-337F8", "SECURE TOKEN-337F16", "SECURE TOKEN-337F32"), виготовлені відповідно до технічних умов ТУ У 26.2-32248356-023:2015, у яких криптографічні перетворення здійснюються програмними модулями та мають значення геш-функцій, що наведені в додатку до цього експертного висновку.

Термін дії експертного висновку – до 11.03.2020.

Перший заступник Голови Служби О.В. Корнейко