



АВТОР
системи інформаційної безпеки

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 компания «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	<ul style="list-style-type: none">• 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)	
Асимметричное шифрование	RSA (512/1024/2048/4096 бит)	
Хеширование	SHA-1, SHA-256	
Возможности встраивания		
Наличие комплекта разработчика	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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
Поддерживаемые ОС	<ul style="list-style-type: none"> • MS Windows 7 (32/64-бит) • MS Windows Vista (32/64-бит) • MS Windows XP (32/64-бит) • MS Windows Server 2008 R2 • MS Windows Server 2008 (32/64-бит) • MS Windows Server 2003 R2 (32/64-бит) • MS Windows Server 2003 (32/64-бит) • Mac OS X (PKCS#11, интерфейс APDU-команд) • Linux (PKCS#11, JCA, интерфейс APDU-команд) 	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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.

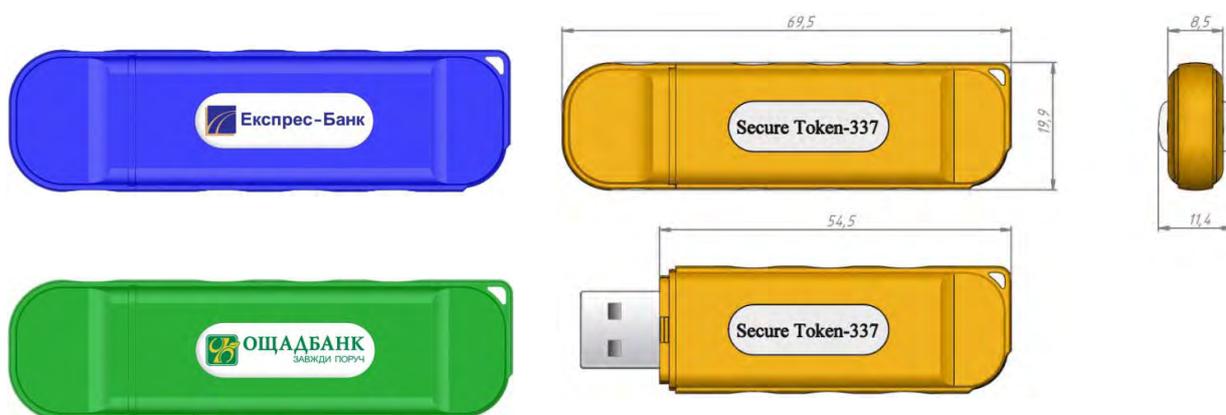
Название стандарта	Длина ключа, бит	Время формирования ЭЦП, мс
ДСТУ 4145-2002	191	30
	257	50
	509	185
PKCS#1 RSA Cryptography Standard	1024	300
	1536	1000
	2048	2000

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 хранения 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»

