Электронные ключи и смарт-карты eToken PRO и NG-OTP

Краткая справочная информация

- **Сводная справочная таблица по USB- ключам и смарт-картам eToken PRO и NG-OTP**
- **Поддержка eToken в продуктах ведущих вендоров**
- **Основные сертификаты совместимости с продуктами ведущих вендоров**
- **Сертификаты на eToken PRO и NG-OTP**
- **Спецификации eToken PRO и NG-OTP**

Для партнеров и корпоративных заказчиков

В данном документе в краткой табличной форме приведена основная справочная информация по электронным USB-ключам и смарт-картам eToken PRO и NG-OTP производства компании Aladdin.

Приведенные данные актуальны по состоянию на март 2006 г.

Aladdin
SECURITY SOLUTIONS
www.aladdin.ru

СОДЕРЖАНИЕ

Сводная справочная таблица по eToken PRO и NG-OTP

Параметр	Краткое описание	
Название, маркировка, варианты исполнения	**eToken PRO** (USB-ключ с памятью 16КБ, 32КБ или 64КБ) **eToken PRO/SC** (смарт-карта с памятью 32КБ или 64КБ) **eToken NG–OTP** (USB-ключ с памятью 32КБ или 64КБ и генератором одноразовых паролей)	
Фото	 eToken PRO (USB-ключ и смарт-карта)	 eToken NG-OTP
Производитель / поставщик, статус	**Aladdin Knowledge System** (Израиль) **Aladdin Software Security R.D.** (дистрибьютор на территории бывшего СССР)	
Ресурс для получения подробной актуальной информации	www.aladdin.ru www.Aladdin.com	
Технология	Смарт-карта / USB-ключ, содержащий микросхему смарт-карты и контроллер USB-порта. USB-ключ подсоединяется напрямую к порту USB компьютера и не требует никаких дополнительных устройств (считывателей). Смарт-карта требует наличия PC/SC-совместимого устройства чтения смарт-карт.	USB-ключ с генератором одноразовых паролей, содержащий микросхему смарт-карты и контроллер USB-порта, не требует для работы дополнительных устройств (считывателей). USB-ключ подсоединяется напрямую к порту USB компьютера и не требует никаких дополнительных устройств (считывателей). Для генерации одноразового пароля достаточно просто нажать кнопку на ключе, не подсоединяя ключ к компьютеру. Значение одноразового пароля отображается на ЖК-дисплее в течение 20 сек.

1. Методы идентификации и аутентификации пользователя

Двухфакторная аутентификация	По наличию eToken и знанию PIN-кода. После ввода PIN-кода сначала происходит авторизация пользователя в операционной системе смарт-карты на уровне приложений с использованием аппаратно реализованных криптографических процедур. После авторизации пользователя становятся доступными операции с закрытыми ключами пользователя, которые используются для аутентификации пользователей в программных системах, поддерживающих аутентификацию пользователей по цифровым сертификатам X.509 v3. Пример: *Smart Card Logon в Windows 2000/XP/2003, приложения, использующие протокол SSL/TLS в режиме двусторонней аутентификации.*	
Аутентификация с использованием одноразовых паролей (one-time passwords, OTP)	eToken PRO совместим с системой RSA SecurID и может использоваться для безопасного хранения SID, используемого для генерации одноразовых паролей.	eToken NG-OTP имеет встроенный генератор одноразовых паролей, оснащен кнопкой для их генерации и дисплеем для отображения. Предназначен для строгой аутентификации пользователя при сетевом доступе к информационным ресурсам (доступ к почте через Microsoft Outlook Web Access, организация VPN-соединения, доступ к Web-серверам) в условиях работы: • на «чужих» компьютерах (гостиницы, аэропорты и др.), где пользователь не имеет возможности установки ПО eToken RTE; • с устройств, не имеющих возможности подключения USB-устройств или смарт-карт (наладонные компьютеры, смартфоны и др.). eToken NG-OTP также работает как обычный eToken PRO при подключении к порту USB компьютера.
Использование идентификатора[1] как средства визуальной идентификации		На смарт-карту eToken PRO/SC может быть нанесена информация о ее владельце и фотография (ID-бэдж) для использования службой безопасности предприятия.

[1] Термин идентификатор используется как обобщающий для всего класса устройств усиленной аутентификации

<table>
<tr><td rowspan="2">Встраивание радио-меток (RFID) для интеграции с системами контроля и управления доступом (СКУД)</td><td> 
</td><td>Налажен выпуск интегрированных (совмещенных) карт в Москве со следующими типами RFID-меток:

HID / SmartProxi ISO, EM-Marine (125 кГц), Cotag (122 / 66 кГц), Ангстрем / БИМ-002 (13,56 МГц).

По требованию заказчика возможен выпуск совмещенных карт с другими типами RFID-меток.</td></tr>
<tr><td>  </td><td>Могут встраиваться любые радио-метки частотой 13,56 МГц и диаметром до 1.2 см. (например, производства HID, EM-Marine, Ангстрем)</td></tr>
</table>

2. Память, криптографические функции	
Размер доступной памяти (EEPROM) для хранения ключевой информации, паролей, профилей и сертификатов с возможностью доступа к ним только авторизованных пользователей	eToken PRO/64K и NG-OTP/64K имеют 64 КБ памяти, из них около 43 КБ доступно для пользовательских данных (в том числе и для защищённых PIN-кодом). eToken PRO/32K и NG-OTP/32K имеют 32 КБ памяти, из них около 24 КБ доступно для пользовательских данных (в том числе и для защищённых PIN-кодом), около 8 КБ занимает операционная система смарт-карты. Доступ к памяти защищен PIN-кодом.
Аппаратная реализация криптографических алгоритмов	В eToken PRO и NG-OTP аппаратно реализованы алгоритмы RSA с длинами ключа 1024 бит и 2048* бит, DSA, DES (ECB, CBC), 3DES (CBC), SHA-1, MAC, iMAC, MAC3, iMAC3, HMAC SHA-1(**). *(*) аппаратная поддержка ключей RSA длиной 2048 бит реализована только для модели eToken PRO/64K* *(**) только в eToken NG-OTP. Этот алгоритм используется при вычислении значения одноразового пароля.*
Аппаратная генерация ключей шифрования и ЭЦП, время	eToken обеспечивает генерацию ключевой пары RSA с длиной ключа 1024 бит менее чем за 10 сек.
Поддержка сертифицированных российских криптографических средств (СКЗИ)	eToken поддерживается в качестве защищенного носителя для ключевых контейнеров: ▪ КриптоПро CSP 3.0 и 2.0 (eToken - рекомендованный носитель) ▪ Signal-COM CSP (eToken - основной носитель) ▪ Верба-OW (eToken - рекомендованный носитель) ▪ Континент-К (один из возможных носителей)
Уровни доступа к памяти и функциональности идентификатора	▪ Гость (доступ на чтение к открытой области памяти, например, ID-номер) ▪ Пользователь (доступ по PIN-коду как открытой, так и защищенной областей памяти, возможность использования eToken для выполнения криптографических операций) ▪ Администратор (доступ по PIN-коду администратора, возможность разблокировать PIN-код пользователя)
Наличие высокоуровневых интерфейсов (PKCS#11, Microsoft CryptoAPI)	eToken имеет удобные средства разработки (SDK), поддерживающие как стандартные интерфейсы (PKCS#11, Microsoft CryptoAPI), так и высокоуровневый специализированный интерфейс Supplimentary API (для работы с функциональностью OTP и мониторинга уровня заряда батарей eToken NG-OTP).

3. Надежность и безопасность	
Уникальность устройства (ID)	Каждый eToken имеет уникальный 6 байтовый серийный номер микросхемы смарт-карты, «прожигаемый» в процессе производства микросхемы. Данный номер не может быть изменён.
Невозможность извлечения ключевой информации	Закрытые ключи, сгенерированные eToken PRO или NG-OTP, или импортированные в него, хранятся в закрытой памяти микросхемы смарт-карты и не могут быть из нее извлечены. Это подтверждается международными сертификатами безопасности ITSEC Level E4, FIPS 140-1 – Level 2, 3.
Защита трафика между устройством и хостом (считывателем / компьютером)	В eToken PRO и NG-OTP предусмотрена возможность шифрования трафика, передаваемого по шине USB, с использованием механизма Secure Messaging по алгоритму 3DES (CBC).
Встроенные механизмы защиты PIN-кода и пароля администратора от подбора	В eToken RTE реализован контроль длины и качества задаваемого пользователем PIN-кода и запрет использования «слабых» комбинаций. При форматировании eToken PRO и NG-OTP имеется возможность задания максимально допустимого количества введённых подряд неправильных значений PIN-кодов пользователя и/или паролей администратора, при достижении которого блокируется доступ к eToken на уровне пользователя / администратора (защита от атаки методом перебора).
Возможность разблокирования устройства администратором безопасности	eToken может быть разблокирован с использованием пароля администратора: ▪ без потери пользовательских данных (смена PIN-кода); ▪ с потерей пользовательских данных (форматирование). С помощью системы централизованного управления eToken TMS операция смены PIN-кода может быть произведена удаленно.
Сертификаты безопасности	▪ Сертификат №925 Гостехкомиссии РФ от 28 июня 2004 года (eToken PRO является программно-аппаратным средством аутентификации пользователей в АС, обрабатывающих конфиденциальную информацию, и может использоваться при проектировании автоматизированных систем до класса защищённости 1Г вкл.) ▪ Сертификат №925/2 ФСТЭК РФ от 25 июля 2005 года (eToken PRO 64K является программно-аппаратным средством аутентификации пользователей в автоматизированных системах, обрабатывающих конфиденциальную информацию, соответствует заданию по безопасности ALD.ETN_PRO_64K.3Б и имеет оценочный уровень доверия ОУД 1 (усиленный) в соответствии с руководящим документом «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Гостехкомиссия России, 2002)) ▪ FIPS 140-1 Level 2 (на весь ключ) ▪ FIPS 140-1 Level 3 (физическая защищенность) ▪ ITSec LE4 (на чип смарт-карты) ▪ ITSec LE4 (на Операционную систему смарт-карты) ▪ ITSec LE4 (на реализацию цифровой подписи) ▪ Common Criteria, уровень – EAL 4+ ▪ Экспертное заключение Службы Безопасности Украины (на соответствие требованиям нормативных документов систем технической защиты информации с уровнем доверия Г2 оценки корректности реализации заявленных функций, на соответствие стандартам реализованных в eToken PRO и RTE 3.0

	криптографических алгоритмов)
Награды, дипломы	▪ «Лучший продукт в области информационной безопасности» (Национальная отраслевая премия по безопасности «ЗУБР-2005») ▪ Лауреат премии «Лучший продукт в области информационной безопасности» (Национальная отраслевая премия по безопасности «ЗУБР-2004») ▪ «Технология 2003 года» - диплом и Памятный знак (Аппарат Совета Безопасности РФ, Комитет Государственной Думы по безопасности, журнал «Бизнес и безопасность в России») ▪ «Информатизация правоохранительных систем - ИПС-2001» - диплом (Академия управления МВД России, Международная Академия информатизации) ▪ «Продукт года» – диплом (Аппарат Совета Безопасности РФ, Комитет Государственной Думы по безопасности, журнал «Бизнес и безопасность в России») ▪ «За достижения в индустрии безопасности» (ITE Group) ▪ 2003—SC Awards Council “Best Encryption Solution” Winner ▪ 2003—Readers Trust Award “Best Encryption Solution” Finalist ▪ 2003—SC Awards Council “Best Communication Security” Highly Commended ▪ 2003—SC Awards Council “Best Access Control” Highly Commended ▪ 2002—Principle Award “Best Security Hardware” Winner ▪ 2002—SC Awards Council “Best Encryption Solution” Highly Commended ▪ 2001—Principle Award “Best Security Hardware” Winner ▪ 2001—Readers Trust Award “Best Encryption Product” Commended
Сертификаты совместимости от ведущих вендоров	▪ Microsoft (Designed for Windows XP, Designed for Windows Server 2003) ▪ Cisco (Cisco Systems Verified, Cisco AVVID Partner) ▪ CA (CA Smart Certified Solution) ▪ Novell (Novell NMAS Partner) ▪ IBM Corporation (Ready for Tivoli) ▪ Check Point Software Technologies (OPSEC Certified) ▪ Entrust (Entrust Ready) ▪ RSA Security (RSA Keon Ready, RSA SecurID Ready, RSA ACE/Server 5 Ready) ▪ SAP AG (SAP Certified Integration) ▪ VeriSign

4. Мобильность и удобство использования	
Требуется ли перезагрузка компьютера после инсталляции драйверов (для ОС Microsoft Windows 2000 / XP / 2003)	Не требуется.
Используются ли дополнительные устройства считывания для подключения идентификаторов к компьютеру (для каких портов, порядок цен)	USB-ключи eToken PRO и NG–OTP напрямую подключаются к порту USB компьютера, дополнительных считывателей не требуется. При использовании смарт-карт eToken PRO требуется любой PC/SC-совместимый ридер, например, ASEdrive, поставляемый компанией Aladdin. При использовании eToken NG-OTP для генерации одноразовых паролей не требуется ни наличие портов, ни драйверов, ни ридеров – сгенерированный одноразовый пароль отображается на дисплее ключа и может быть введен в компьютер или PDA через клавиатуру или перьевой ввод.
Мобильность работы (возможность быстрого перехода на другое рабочее место без ручного копирования и установки пользовательских профилей, сертификатов)	В составе eToken RTE реализован провайдер хранилища сертификатов X.509 (CertStore Provider), что обеспечивает мобильность пользователей: при подключении eToken хранящиеся в его памяти сертификаты стандарта X.509 автоматически копируются из хранилища сертификатов eToken в хранилище сертификатов «Личные». Закрытые ключи всегда остаются в памяти eToken.

5. Интеграция с УЦ, централизованное администрирование, средства разработки

Поддержка Удостоверяющими Центрами мировых и российских производителей	eToken корректно работает и обеспечивает возможность выписки и хранения нескольких сертификатов в свою защищенную память для Microsoft CA (Windows 2000, 2003 Server), КриптоПро УЦ, RSA Keon, VeriSign, Thawte, Entrust, Globalsing, GTE CyberTrust и имеет соответствующие сертификаты совместимости от производителей.
Наличие системы централизованного контроля и управления идентификаторами, обработки потерянных или вышедших из употребления идентификаторов, дистанционного восстановления данных в памяти идентификаторов	eToken TMS (Token Management System), производитель – Aladdin Knowledge Systems.
Наличие средств разработки (SDK), поддержка языков программирования	eToken имеет удобное средство разработки (eToken SDK), обеспечивающее возможность работы с eToken через: • высокоуровневые интерфейсы прикладного программирования Microsoft CryptoAPI и PKCS#11; • 16-битовые библиотеки, предназначенные для создания решений по защите компьютера от несанкционированной начальной загрузки и аутентификации пользователя перед загрузкой операционной системы; • высокоуровневый специализированный интерфейс Supplimentary API для работы с функциональностью генерации OTP и мониторинга уровня заряда батарей eToken NG-OTP. Также в состав eToken SDK входят обучающие материалы, примеры исходных кодов и программ, которые можно модифицировать и использовать в разработке собственных приложений. Актуальная версия eToken SDK 3.60 поддерживает платформы Microsoft Windows, Linux, MAC OS X и реальный режим работы процессора (для создания 16-битовых приложений, выполняющихся до загрузки операционной системы компьютера). Языки программирования: C++, C, VB, Java, Delphi.
Поддерживаемые платформы	• Microsoft Windows 98 / Me / NT / 2000 / XP / 2003 • Windows XP Embedded, Windows CE (для терминальных станций) • Linux (Red Hat, SuSE, Fedora) • MAC OS X 10.4 • Инструментарий для поддержки eToken до начала загрузки ОС.

6. Инфраструктура	
Возможность крупных поставок (до десятков тысяч) в ограниченные сроки	Да, есть опыт производства и поставки партий размером до 50,000 шт. в течение двадцати дней.
Наличие склада, возможность поставки ограниченных по количеству партий (от 1 до 1000 шт.) в день обращения	Да, со склада в Москве.
Техническая поддержка от производителя/поставщика на русском языке	Есть.
Наличие команды разработчиков в России, имеющих опыт разработки продуктов с использованием eToken	Aladdin имеет собственный отдел разработки в г.Москве), который может высококачественно и в сжатые сроки выполнить в соответствии с требованиями заказчика разработку нового продукта или провести доработку имеющегося для его полного соответствия требованиям конкретного заказчика. Aladdin предлагает консалтинговые услуги для партнеров - разработчиков продуктов и решений с использованием eToken. Aladdin имеет опыт выпуска собственный продуктов (более 20) с использованием eToken, среди них: Secret Disk NG, линейка продуктов SecurLogon (для Oracle, Novell), разработки драйверов eToken для Embedded XP / CE и др., опыт встраивания российских средств криптографической защиты (СКЗИ) в продукты западных производителей (например, Novell GroupWise).
Наличие необходимых лицензий у поставщика, разрешений на экспорт/импорт устройств	Aladdin имеет все необходимые лицензии ФСБ и Гостехкомиссии РФ на деятельность в области разработки, производства, оказания услуг, распространения СКЗИ и защищенных систем (не включая защиту сведений, составляющих гостайну), а также необходимые разрешения ФСБ на ввоз/вывоз eToken.
Сертификаты на eToken (отсутствия вредных веществ, пожаробезопасности, отсутствия вредных электромагнитных излучений, влагозащищённости, санэпидемиологической службы и пр.)	▪ eToken имеет заключение санэпидемиологической службы России и международный сертификат Environmental certificate EU 67_548 и признан безопасным для здоровья человека. ▪ eToken успешно прошел тесты UL 94 на воспламеняемость пластических материалов, применяемых в устройствах и приборах. eToken соответствуют нормам UL 1950, применяемым к IT-оборудованию, и имеет Сертификат лаборатории по технике безопасности США (UL). ▪ eToken был протестирован и признан соответствующим международным требованиям к цифровым устройствам класса «B» согласно Части 15 норм FCC. Соответствие уровня электромагнитных излучений требованиям FCC Class 15, Subpart B, Class B. Сертификат Федеральной комиссии связи США (FCC). ▪ eToken обладает водонепроницаемым корпусом, допускается погружение в воду на глубину до 2 метров и имеет международный сертификат IEC 529 IP X38.
Наличие интеграторов, имеющих опыт и специалистов по внедрению крупных проектов (более 500 мест) с использованием данного типа идентификаторов	Aladdin имеет более 60 партнеров по внедрению, среди них ведущие интеграторы: Крок, Инфосистемы Джет, Ланит, Элвис-Плюс, ICL КПО и др.
Рекомендованная розничная цена	$44-47 (на USB-ключ eToken PRO с памятью 16/32 КБ). $45-55 (на USB-ключ eToken PRO с памятью 64 КБ, в зависимости от размера поставки). $56-69 (на USB-ключ eToken NG-OTP с генератором одноразовых паролей и памятью 64 КБ, в зависимости от размера поставки). $16-22 (на смарт-карту eToken PRO с памятью 32 КБ, в зависимости от размера поставки).

Поддержка eToken PRO и NG-OTP в продуктах ведущих вендоров

Обозначения

○	Не поддерживается.
✷	Декларируется, что поддерживается, но тестирование не проводилось. Документации по встраиванию и использованию нет.
●[i]	Поддерживается. Есть документация по встраиванию и использованию. Сертификатов совместимости нет. *Index – Поддержка обеспечивается установкой дополнительного клиентского ПО.*
■	Поддерживается штатными средствами, установка дополнительного клиентского ПО не требуется. Есть документация по встраиванию и использованию. Есть сертификат совместимости производителя или рекомендация на использование идентификатора от вендора продукта.

Вендор	Продукт	eToken PRO
Популярные продукты[2] западных вендоров		
Apache Software Foundation	APACHE Web Server	●
Adobe Systems Inc.	Adobe Acrobat (версии 5.0 или выше)	■
CA	CA eTrust SSO (Single Sign-On)	■
Check Point Software Technologies	Check Point VPN-1 (версии 4.1 и NG)	■
Cisco Systems	Cisco ACS SecureServer	●
	Cisco Aironet Access Point	●
	Cisco PIX Firewall	●
	Cisco VPN 3000 Concentrator Series	■
	Cisco VPN Client	■
Citrix	Citrix MetaFrame Access Suite	●
IBM Corporation	IBM Lotus Notes (версии 4.6 и выше)	●[i]
	IBM Lotus Notes/Domino 6	●
	IBM Tivoli Access Manager	■
	IBM WebSphere	●
Oracle	Oracle DBMS (версия 8.1.7 и выше)	●
Linux	ASP Linux 7.2 и выше Red Hat Linux 8.x и выше	●[i]

[2] В данной таблице приведено менее половины всех поддерживаемых продуктов. Полный перечень см. на сайте www.eAladdin.com

Вендор	Продукт	eToken PRO
	SuSE Linux 8.2 и выше Fedora Core	
Microsoft	Microsoft Exchange Server 2000/2003	●
	Microsoft Internet Information Server (IIS)	●
	Microsoft Outlook	●
	Microsoft Terminal Services	●
	Microsoft Windows XP[3]	■
	Microsoft Windows Server 2000/2003	●
	Microsoft Windows XP Embedded	●
SAP AG	mySAP Enterprise Portal	■
	SAP R/3	●[4]
Nortel Networks	Nortel Contivity VPN 600	■
Novell	Novell eDirectory (версия 8.5 и выше)	●
	Novell iChain	●
	Novell GroupWise (версия 6.5 и выше)	●
PGP Corporation	PGP	■
RSA Security	RSA ACE/Server	■
Control Break International	SafeBoot	■
SSH	Secure Shell	■
Ritlabs	The Bat! Professional Edition	■
Удостоверяющие центры, PKI		
CA	CA eTrust PKI	■
Entrust	Entrust/PKI	■
Netscape	iPlanet Certificate Management System	✷
Microsoft	Microsoft CA	■
RSA Security	RSA Keon CA	■
VeriSign	Site Trust Services	■
Крипто-Про	Удостоверяющий центр	■
Валидата	Удостоверяющий центр CCERT PKI	■
Валидата и МО ПНИЭИ	Удостоверяющий центр VCERT PKI	■
Валидата	ЦС и ЦР ПКЗИ СЭД ММВБ	■

[3] eToken PRO входит в Базовую и Полную поставки сертифицированной версии Windows XP

Вендор	Продукт	eToken PRO
Валидата и МО ПНИЭИ	ЦС и ЦР СКАД Сигнатура/СКЗИ Янтарь-АСБР для Банка России	■
Новый Адам	Криптографический Центр Акей	●
Популярные[4] продукты российских разработчиков		
АстроСофт Девелопмент	Astrosoft Protected Office	■
Борлас Ай-Би-Си	AC+	■
Информзащита	Континент-К	●
Инфосистемы Джет	Тропа Джет	■
Инфотекс	ViPNet	●
Крипто-Про	КриптоПро CSP	■
ЛанКрипто	ЛАН Крипто провайдер	●
ЛИССИ	Shield Channel-FW	●
МО ПНИЭИ	СКЗИ Верба - W	●
ОКБ САПР	Аккорд-АМДЗ	✷
Сигнал-Ком	Signal-COM CSP	■
	Крипто-КОМ 3.1	●
Элвис-Плюс	Застава 3.3	■
Валидата	VCERT PKI и продукты линейки Курьер-VCERT	●
Валидата	CCERT PKI и продукты линейки Курьер-CCERT	■
Валидата	ПКЗИ СЭД ММВБ и приложения CMA Small Systems A.B. для РП ММВБ	■
Валидата и МО ПНИЭИ	СКАД Сигнатура/СКЗИ Янтарь-АСБР для Банка России	■
Электронные Офисные Системы	Система ДЕЛО	■

[4] В данном разделе приведено менее половины всех продуктов, поддерживающих eToken. Для получения более подробной информации обратитесь к производителю интересующего вас продукта или в компанию Aladdin.

Основные сертификаты совместимости

ОСНОВНЫЕ СЕРТИФИКАТЫ СОВМЕСТИМОСТИ С ПРОДУКТАМИ ВЕДУЩИХ ВЕНДОРОВ		
CA Smart Certified Solution		USB-ключи и смарт-карты eToken сертифицированы на совместимость с продуктами eTrust PKI (службы и сервисы для построения инфраструктуры открытых ключей) и eTrust Single Sign-On (решение для обеспечения единой точка входа пользователя в информационные системы). http://www3.ca.com/partners/solution/Partner.asp?CID=30547
Cisco AVVID Partner (Cisco)		С июня 2002 года компания Aladdin является участником программы Cisco AVVID Partner Program по направлению «Identity» (Контроль доступа). Тесное технологическое партнёрство компаний обеспечивает полную совместимость eToken с технологиями аутентификации, используемыми в продуктах Cisco: VPN 3000 Concentrator Series, ACS SecureServer, PIX Firewall, VPN Client. http://www.cisco.com/pcgi-bin/ecoa/displayProfile?PARTNER_ID=11564
Cisco Systems Verified (Cisco)		USB-ключи и смарт-карты eToken обеспечивают строгую двухфакторную аутентификацию пользователей при доступе к сетевым ресурсам и приложениям. В памяти eToken хранятся ключевые пары и сертификаты, используемые на фазе 1 аутентификации по протоколу IPSec, называемой IKE (Internet Key Exchange). http://www.cisco.com/pcgi-bin/ecoa/displayProfile?PARTNER_ID=11564
Designed for Windows XP (Microsoft Corporation)		Сертификат подтверждает стабильную и бесперебойную работу электронных ключей eToken на компьютерах под управлением Windows XP. Служба Windows Update теперь автоматически отслеживает выход обновленных версий драйверов eToken. Это значительно упрощает процесс корпоративного развёртывания eToken, снижает затраты на сопровождение и поддержку. http://www.microsoft.com/windows/catalog/default.aspx?subid=22&xslt=categoryl3&pgn=7d15bd26-ea50-47b4-91c6-1fdafaa11ec9&tab=3
Entrust Ready (Entrust)		USB-ключи eToken PRO совместимы с Entrust Authority Security Manager 6.0, Entrust Entelligence Desktop Manager 6.1 и Entrust Entelligence Security Provider 7.0. http://www.entrust.com/news/files/01_15_03.htm http://www.entrust.com/partners/solutions/30.htm
Novell NMAS Partner (Novell)		USB-ключи и смарт-карты eToken обеспечивают строгую двухфакторную аутентификацию пользователей при доступе к серверам Novell Netware и службе каталога Novell eDirectory. eToken также используется для аутентификации пользователей при доступе к защищённым Web-серверам на основе Novell iChain, защиты электронной почты и ЭЦП в почтовой системе Novell GroupWise, аутентификации пользователей при организации VPN-соединений на основе Novell Border Manager. *Компания Aladdin – единственный среди производителей USB-ключей, имеющий статус Novell NMAS Partner.* http://www.novell.com/products/nmas/partners/UU
OPSEC Certified (Check Point Software Technologies)		USB-ключи eToken PRO поддерживают Check Point VPN-1/FireWall-1 Next Generation (NG) через интерфейс OPSEC (Open Platform for Security) NG. eToken PRO может использоваться с продуктами Check Point NG VPN-1 SecureClient и SecuRemote. http://www.checkpoint.com/press/partners/2002/aladdin021802.html
Ready for Tivoli (IBM Corporation)		USB-ключи eToken PRO могут использоваться с программным обеспечением IBM Tivoli. http://www.developer.ibm.com/solutions/isv/igssg.nsf/list/bycompanyname/86256B7C0019CE5B86256D01003A3AD9?OpenDocument http://www.developer.ibm.com/solutions/isv/igssg.nsf/list/bycompanyname/86256B7C0019CE5B86256D01003A2D7C?OpenDocument

ОСНОВНЫЕ СЕРТИФИКАТЫ СОВМЕСТИМОСТИ С ПРОДУКТАМИ ВЕДУЩИХ ВЕНДОРОВ		
RSA Keon Ready RSA SecurID Ready RSA ACE/Server 5 Ready (RSA Security)		USB-ключи eToken PRO совместимы с системами RSA Keon, RSA SecurID и RSA ACE/Server 5.x. http://rsasecurity.agora.com/rsasecured/detail.asp?product_id=942 http://rsasecurity.agora.com/rsasecured/detail.asp?product_id=1155
SAP Certified Integration (SAP AG)		Центр Интеграции и Сертификации компании SAP AG (Вальдорф, Германия) сертифицировал электронные ключи eToken PRO на совместимость с ERP-системой SAP R/3 и порталом mySAP Enterprise Portal. eToken стал первым сертифицированным средством для строгой двухфакторной аутентификации пользователя при доступе к приложениям и данным SAP - как через собственный графический интерфейс SAP GUI, так и через стандартный Web-интерфейс. eToken используется для генерации ключевых пар, хранения цифровых сертификатов, аутентификации пользователей и защиты передаваемых по сети данных по протоколам SSL и SNC (Secure Network Connection). http://www.sap.com/partners/netweaver.asp
VeriSign		Компания Aladdin является технологическим партнёром VeriSign по направлениям «Authentication and Digital Identity», «Smart Card Management» и «Smart Card Solutions». Электронные ключи и смарт-карты eToken предоставляют пользователям услуг VeriSign возможности локальной аппаратной генерации ключей шифрования и ЭЦП, надёжного хранения изданных VeriSign цифровых сертификатов, а также обеспечивают простоту и надёжность их использования со всеми приложениями. http://www.verisign.com/cgi-bin/partnernet/se/showProfile.cgi?co=Aladdin%20Knowledge%20Systems%20Ltd.&ca=Authentication%20and%20Digital%20IdentitySmart%20Card%20ManagementSmart%20Card%20Solutions

Сертификаты на eToken PRO и NG-OTP

СЕРТИФИКАТЫ БЕЗОПАСНОСТИ		
Сертификат №925 Гостехкомиссии РФ, выдан 28 июня 2004	*копия документа выдается по запросу*	USB-ключи и смарт-карты eToken PRO с памятью 32КБ являются программно-аппаратным средством аутентификации пользователей в автоматизированных системах (АС), обрабатывающих конфиденциальную информацию, и могут использоваться при проектировании АС до класса защищенности 1Г включительно.
Сертификат №925/2 ФСТЭК РФ, выдан 25 июля 2005 года	*копия документа выдается по запросу*	USB-ключи и смарт-карты eToken PRO с памятью 64КБ является программно-аппаратным средством аутентификации пользователей в автоматизированных системах, обрабатывающих конфиденциальную информацию, соответствует заданию по безопасности ALD.ETN_PRO_64K.3Б и имеет оценочный уровень доверия ОУД 1 (усиленный) в соответствии с руководящим документом «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Гостехкомиссия России, 2002)
ITSEC Level E4 ITSEM Level E4	*копия документа выдается по запросу*	Сертификат на используемую в eToken микросхему смарт-карты Infineon SLE66CX320P. Тестировались следующие функции подсистемы безопасности: самодиагностика устройства, шифрование данных с использованием встроенных механизмов управления ключами и генерации случайных чисел, защита от несанкционированного доступа.
ITSEC Level E4 ITSEM Level E4	*копия документа выдается по запросу*	Сертификат на операционную систему Siemens CardOS/M4.01 и механизм формирования ЭЦП. Тестировались следующие функции подсистемы безопасности: идентификация и аутентификация, контроль доступа, аудит, обмен данными, повторное использование данных.
FIPS 140-1 – Level 2, 3		Сертификат на соответствие требованиям FIPS (Federal Information Process Standards) второго и третьего уровня физической защиты: • FIPS 140-1 Level 2 (весь ключ) • FIPS 140-1 Level 3 (физическая защищенность корпуса) http://www.ealaddin.com//news/2003/etoken/FIPS.asp
Common Criteria		Уровень – EAL 4+
Экспертное заключение Службы Безопасности Украины	*копия документа выдается по запросу*	Сертификат на соответствие требованиям нормативных документов СТЗИ (систем технической защиты информации) с уровнем доверия Г2 оценки корректности реализации заявленных функций в eToken PRO и RTE 3.0. http://eToken.com.ua
Экспертное заключение Службы Безопасности Украины (от 25.09.03)	*копия документа выдается по запросу*	Сертификат на соответствие стандартам реализованных в eToken PRO и RTE 3.0 криптографических алгоритмов: • аппаратно реализованные алгоритмы RSA, DES, 3DES соответствуют стандартам RFC-2437 и DES-FIPS Pub 46-3 (CBC); • аппаратно реализованный алгоритм SHA-1 соответствует стандарту FIPS Pub 180-1; • программно реализованные алгоритмы MD-5, HMAC соответствуют стандартам RFC-1321 и Microsoft Base crypto-provider. http://eToken.com.ua

СЕРТИФИКАТЫ КАЧЕСТВА ПРОДУКТОВ и УСЛУГ		
Соответствие системы контроля качества продукции требованиям ISO 9001:2000		Дата первоначальной сертификации: 26.10.1997 Подтверждение сертификации: 2000, 2003 гг. Действительно до: 31.03.2006.
IQ Net - Certified Quality System SI 2002 ISO 9002		Вся продукция eToken разработана и выпускается компанией Aladdin Knowledge Systems, сертифицированной по ISO 9002. Система обеспечения качества Aladdin одобрена Международной организацией по стандартизации (ISO).
Certified for Europe (декларация производителя)		eToken соответствует Директиве CE EMC и соответствующим стандартам (EMC директива 89/336/EEC и соответствующие стандарты EN 55022, EN 50082-1). eToken маркируется логотипом CE, сертификат CE включается в каждую поставку eToken или выдается по запросу.
Environmental certificate EU 67_548 (декларация производителя)	*копия документа выдается по запросу*	Отсутствие содержания вредных веществ или их содержание в пределах санитарно-гигиенических норм.
Заключение санэпидемиологической службы России	*копия документа выдается по запросу*	Безопасность изделий для здоровья человека.
USB-IF Certificate (альянс производителей USB-устройств)		Соответствие ключей eToken стандартам USB 1.1 и 2.0. Aladdin входит в альянс производителей USB-устройств. http://www.usb.org/app/vendors/
FCC Class 15, Subpart B, Class B	*копия документа выдается по запросу*	Соответствие уровня электромагнитных излучений требованиям FCC Class 15, Subpart B, Class B.
Среднее время наработки на отказ (MTBF) (декларация производителя)	*копия документа выдается по запросу*	Среднее время наработки на отказ для моделей eToken R2 и PRO, смарт-карт составляет свыше 1000 лет.
UL		eToken успешно прошел тесты UL 94 на воспламеняемость пластических материалов, применяемых в устройствах и приборах (UL 94 Tests for Flammability of Plastic Materials for Parts in Devices and Appliances). eToken соответствует нормам UL 1950 (UL 1950 Safety of Information Technology Equipment regulations).
EC 529 IP X8	*копия документа выдается по запросу*	Сопротивляемость воде – допускается погружение в воду на глубину до 2 метров.

Спецификация eToken PRO

Фотография	 USB-ключ и смарт-карта eToken		
Архитектура*	Смарт-карта со встроенной EEPROM памятью и защищенный микроконтроллер, реализующий функциональность PC/SC считывателя		
Модели	eToken PRO/16K	eToken PRO/32K	eToken PRO/64K
Размер EEPROM- памяти	16 КБ	32 КБ	64 КБ
Исполнение*	USB-ключ	USB-ключ или смарт-карта	USB-ключ или смарт-карта
Поддерживаемые ОС	• Microsoft Windows 98 / Me / NT / 2000 / XP / 2003 • Windows XP Embedded, Windows CE (для терминальных станций) • Linux (Red Hat, SuSE, Fedora) • MAC OS X 10.4 • Инструментарий для поддержки eToken до начала загрузки ОС.		
Интерфейсы прикладного программирования (API) и стандарты	PKCS#11 v2.01, Microsoft CryptoAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE, Siemens/Infineon APDU команды		
Сертификаты безопасности*	ITSEC Level E4, FIPS 140-1 – уровни 2, 3		
Аппаратно реализованные алгоритмы	RSA/1024, DES, TripleDES, SHA-1, MAC, iMAC [DSA и MD-5 - по запросу]		RSA/2048, RSA/1024, DES, TripleDES, SHA-1, MAC, iMAC
Программно реализованные алгоритмы	MD5, MD5 HMAC		
Генерация ключевой пары RSA 1024 бит	< 10 сек.		
Формирование ЭЦП с использованием RSA 1024 бит	< 1 сек.		
Световой индикатор режимов работы*	Включен / Выключен / Мигает		
Чип смарт-карты	Infineon SLE66CX160S	Infineon SLE66CX320P	Infineon SLE66CX642P
Операционная система смарт-карты	CardOS/M4	CardOS/M4.01	CardOS V4.2
Тактовая частота процессора	6 МГц		
USB протокол*	USB версии 1.1, скорость передачи данных до 1,5 Мб/с		USB версии 2.0, скорость передачи данных до 1,5 Мб/с

Тип микроконтроллера*	CYPRESS CY63001A		CYPRESS CY7C63723-SC
ATR*	3B E2 00 FF C1 10 31 FE 55 C8 02 9C	3B F2 98 00 FF C1 10 31 FE 55 C8 03 15	3B F2 18 00 FF C1 0A 31 FE 55 C8 06 8A
Поддержка Reset и «спящего» режима USB (Suspend mode)*	Да		
Потребляемая мощность*	< 120 мВт		
Внутренний источник питания	Отсутствует		
Интерфейс / Разъем*	USB type A		
Размеры*	47 x 16 x 8 мм		
Вес*	~5 г		
Рабочая температура	От 0 до 70 °C		
Температура хранения	От -40 до +85 °C		
Влажность	0 - 100% без конденсата		
Производство	Собственное, сертифицированное по ISO 9002 (Израиль)		
Поддержка Plug & Play	Да		
Среднее время наработки на отказ (MTBF)	Не менее 1,000 лет		
Срок хранения данных в памяти	Минимум 10 лет		
Количество перезаписей в одну ячейку памяти	Минимум 500,000 раз		
Гарантийный срок	12 месяцев		

* - *только для USB-исполнения*

Спецификация eToken NG-OTP

Фотография		
Архитектура	Смарт-карта со встроенной EEPROM памятью, генератором одноразовых паролей и защищенным микроконтроллером, реализующим функциональность PC/SC считывателя	
Модели	eToken NG-OTP/32K	eToken NG-OTP/64K
Размер EEPROM- памяти	32 КБ	64 КБ
Исполнение	USB-ключ в пластиковом корпусе с кнопкой для генерации одноразовых паролей и жидкокристаллическим дисплеем	
Поддерживаемые ОС	• Microsoft Windows 98 / Me / NT / 2000 / XP / 2003 • Windows XP Embedded, Windows CE (для терминальных станций) • Linux (Red Hat, SuSE, Fedora) • MAC OS X 10.4 • Инструментарий для поддержки eToken до начала загрузки ОС.	
API и стандарты	PKCS#11 v2.01, Microsoft CryptoAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE, Siemens/Infineon APDU команды	
Сертификаты безопасности	Common Criteria EAL 4+ (на микросхему смарт-карты)	
Аппаратно реализованные алгоритмы	RSA/1024, DES, TripleDES, SHA-1, HMAC SHA-1 (используется при генерации одноразового пароля), MAC, iMAC	
Алгоритм генерации одноразовых паролей	Совместимый с реализацией OATH (на основе HMAC SHA-1)	
Программно реализованные алгоритмы	MD5, MD5 HMAC	
Генерация ключевой пары RSA 1024 бит	< 10 сек.	
Формирование ЭЦП с использованием RSA 1024 бит	< 1 сек.	
Световой индикатор режимов работы	Включен / Выключен / Мигает	
Чип смарт-карты	Infineon SLE66CX322P	Infineon SLE66CX642P
Операционная система смарт-карты	Siemens CardOS V4.2	
Тактовая частота процессора	6 МГц	
USB протокол	USB версии 2.0, скорость передачи данных до 12 Мб/с	
Тип микроконтроллера	Cygnal C8051F321	
ATR*		3B F2 18 00 FF C1 0A 31 FE 55 C8 06 8A
Поддержка Reset и «спящего» режима USB (Suspend mode)	Да	
Потребляемая мощность	< 120 мВт	

Внутренний источник питания	2 заменяемые литиевые батареи.
Гарантированное количество генераций одноразовых паролей и их отображений каждого из них в течение 20 сек., от одного комплекта батарей	14.000 (более 12 лет эксплуатации при ежедневном использовании 3 одноразовых паролей).
Интерфейс / Разъем	USB type A
Размеры	70 x 28 x 10,5 мм, видимая площадь ЖК-дисплея 30 x 8 мм
Вес	17 г
Рабочая температура	От 0 до 65 °C
Температура хранения	От -20 до +65 °C
Влажность	0 - 95% без конденсата
Производство	Собственное, сертифицированное по ISO 9002 (Израиль)
Поддержка Plug & Play	Да
Срок хранения данных в памяти	Минимум 10 лет
Количество перезаписей в одну ячейку памяти	Минимум 500,000 раз
Гарантийный срок	12 месяцев