Технические спецификации

Объем защищенной памяти	72 КБ на микросхеме смарт-карты
Поддерживаемые ОС	Microsoft Windows 2000/2003/XP/Vista/2008/2008 R2/7 (32 и 64-битные версии); Linux; Mac OS Одноразовые пароли могут использоваться в любой операционной среде
Срок хранения данных в памяти	Не менее 10 лет
Количество циклов перезаписи памяти	Не менее 500,000

Централизованное управление

eToken TMS (Token Management System)/SAM (SafeNet Autentication Manager)

TMS/SAM – решение для построения инфраструктуры безопасного доступа к информационным ресурсам предприятия с централизованным управлением. SAM является новым поколением системы централизованного управления персональными средствами аутентификации и хранения ключевой информации TMS.

Назначение

- Централизованное управление жизненным циклом средств аутентификации (инициализация / выпуск сертификата, ввод в эксплуатацию, обслуживание, вывод из эксплуатации / блокирование).
- Учет средств аутентификации, аудит их использования.
- Автоматизация типовых операций и сценариев администрирования в соответствии с политиками безопасности организации.
- Быстрое и самостоятельное решение проблем пользователей без обращения к администраторам.

Для расширения возможностей TMS/SAM доступен комплект разработчика Connector SDK, позволяющий добавить возможность работы со сторонними приложениями в процессе стандартных операций с устройствами eToken (добавление, назначение, отзыв и т.д.).

Сертифицированные USB-ключи и смарт-карты

Сертифицированные электронные ключи eToken являются программно-аппаратным средством аутентификации и хранения ключевой информации и средством защиты информации от несанкционированного доступа (сертификат ФСТЭК России №1883 от 11.08.2009 г. продлен до 11.08.2013 г.).
В соответствии с рекомендациями руководящих документов сертифицированные электронные ключи eToken могут использоваться в ИСПДн до 1 класса включительно и для создания автоматизированных информационных систем до класса защищенности 1Г включительно.

Сертифицированные электронные ключи eToken являются рекомендуемым носителем ключевой информации для сертифицированных СКЗИ российских разработчиков.

Электронный ключ eToken ГОСТ соответствует требованиям ФСБ России к СКЗИ класса КС2 и может использоваться для защиты информации, не содержащей сведений, составляющих государственную тайну (Сертификат соответствия № СФ/124-1671 от 11 мая 2011 г.).

Возможности кастомизации

- **Интеграция с системами контроля доступа** – все USB-ключи и смарт-карты могут выпускаться со встроенными пассивными радио-метками RFID для контроля доступа сотрудников в помещения.
- **Корпуса с логотипом** – возможно изготовление корпусов USB-ключей с объемным логотипом заказчика.
- **Печать логотипа заказчика** – на USB-ключи возможно нанесение логотипа заказчика методом тампопечати, на смарт-карты возможно нанесение фотографии сотрудника, либо логотипа организации.
- **Различные цвета корпуса** – по желанию заказчика USB-ключи могут быть выполнены в корпусе другого цвета.

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (продлены до 18.02.13), № 2874 от 18.05.12
Лицензии ФСБ России № 9333 Р от 03.09.10, №12052 П от 05.04.12 и № 18229 от 13.10.10
Сертификат соответствия СМК ГОСТ Р ИСО 9001-2008 № РОСС RU.ИС72.К00069 от 16.07.12
Microsoft Silver OEM Hardware Partner, Oracle Gold Partner

+7 (495) 223-00-01; aladdin@aladdin-rd.ru; www.aladdin-rd.ru

ID: 4123-092012

Решения для аутентификации и формирования ЭП: смарт-карты и USB-токены

- **Строгая двухфакторная аутентификация** пользователей при доступе к защищенным ресурсам (компьютерам, сетям, приложениям)
- **Аппаратное выполнение криптографических операций** в доверенной среде (в микросхеме ключа: генерация ключей шифрования, симметричное и асимметричное шифрование, вычисление хэш-функции, выработка электронной подписи)
- **Безопасное хранение критически важных данных** – криптографических ключей, профилей пользователей, настроек приложений, цифровых сертификатов и пр. в энергонезависимой памяти ключа
- **Сертифицированные версии** для защиты информации в АС до класса защищенности 1Г включительно и для защиты персональных данных в ИСПДн до 1 класса включительно

Аладдин РД
www.aladdin-rd.ru

Электронные ключи eToken могут использоваться в любых приложениях для замены парольной защиты на более надежную двухфакторную аутентификацию.

Например, если для аутентификации пользователю необходимо предоставить USB-ключ и ввести пароль, то злоумышленник не сможет получить доступ к данным, так как ему нужно не только подсмотреть пароль, но и предъявить физическое устройство, кража которого быстро обнаружима.

Модельный ряд

eToken PRO (Java)

eToken PRO (Java) – персональное средство аутентификации и защищенного хранения пользовательских данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной подписью, выпускается в виде USB-ключа и смарт-карты.

eToken PRO (Java) является следующим поколением электронных ключей eToken PRO. По сравнению с ними eToken PRO (Java) имеет увеличенный объем памяти для защищенного хранения пользовательских данных и предоставляет возможность расширения функционала за счет загрузки дополнительных приложений (Java - апплетов).

Рекомендуется для решения следующих задач корпоративных заказчиков:

- обеспечение строгой двухфакторной аутентификации пользователей в операционных системах и бизнес-приложениях (Microsoft, Citrix, Cisco Systems, IBM, SAP, Check Point), защищенное хранение ключевой информации российских СКЗИ (КриптоПро CSP, Крипто-КОМ, Домен-К, Верба-OW и др.);
- защита ключей электронной подписи пользователей в системах электронного документооборота, формирование электронной подписи документов и транзакций, обеспечение безопасной работы с электронной почтой;
- защита закрытых ключей электронной подписи пользователей систем дистанционного банковского обслуживания.

Смарт-карты eToken PRO (Java) со встроенными радио-метками RFID, напечатанным логотипом компании, фотографиями сотрудников могут использоваться в качестве единых карт для контроля физического доступа в помещения и контроля логического доступа к информационным ресурсам.

eToken PRO Anywhere

eToken PRO Anywhere – USB-ключ для безопасного доступа к Web-ресурсам с любого компьютера без предварительной установки ПО.

eToken PRO Anywhere предоставляет следующие сервисы безопасности:

- автоматический запуск браузера и открытие заранее заданных Web-сайтов, адреса которых хранятся в защищенной памяти устройства;
- аутентификация пользователя в рамках протокола SSL/TLS и защита всех данных, передаваемых по сети Интернет;
- защита от фишинга и атак «человек посередине».

Рекомендуется:

- поставщикам on-line услуг для предоставления клиентам безопасного доступа к Web-ресурсам без установки клиентского ПО;
- организациям – для предоставления своим сотрудникам удаленного доступа к корпоративным порталам и электронной почте с возможностью использовать электронной подписи с любых компьютеров;
- для снижения нагрузки на службы технической поддержки по вопросам удаленного доступа.

eToken NG-FLASH (Java)

eToken NG-FLASH (Java) – комбинированный USB-ключ, обладающий функциональными возможностями eToken PRO (Java), и оснащенный дополнительным модулем Flash-памяти объемом до 16 ГБ.

Дополнительная Flash-память устройства позволяет хранить данные в зашифрованном виде и может быть использована для:

- доверенной загрузки операционных систем Microsoft Windows или Linux (образ операционной системы записывается в память устройства);
- хранения и запуска предварительно сконфигурированной виртуальной машины (VMWare, Virtual PC) с предустановленным набором ПО и настроенными параметрами безопасности;
- автоматического запуска приложений из памяти устройства;
- безопасного хранения, транспортировки и резервного копирования данных;
- запуска безопасного предварительно настроенного браузера.

Рекомендуется:

- администраторам безопасности, аудиторам ИБ – для создания временных центров по оценке защищенности информационных систем, оценке их соответствия требованиям нормативных документов;
- компаниям, работающим через агентскую сеть (страхование, кредитование) – для создания агентских рабочих мест по обслуживанию клиентов;
- разработчикам ПО – для распространения / тиражирования программного обеспечения;
- всем пользователям – для безопасного хранения, транспортировки и резервного копирования данных.

eToken PASS

eToken PASS – автономный генератор одноразовых паролей, не требующий подключения к компьютеру. Является более дешевой альтернативой eToken NG-OTP (Java), без возможности использования в PKI-системах.

Рекомендуется:

- банкам, кредитно-финансовым организациям – для повышения уровня доступности предоставляемых ими сервисов, повышения удовлетворенности клиентов качеством обслуживания;
- разработчикам систем ДБО – для создания конкурентоспособных систем ДБО, позволяющих банкам, использующим эти системы, повышать уровень доступности предоставляемых услуг;
- поставщикам on-line услуг – для аутентификации доступа подписчиков и максимального расширения аудитории;
- пользователям мобильных устройств (телефонов, смартфонов, коммуникаторов).

eToken NG-OTP (Java)

eToken NG-OTP (Java) – комбинированный USB-ключ с генератором одноразовых паролей (One-Time Password – OTP). Обладает всем функционалом eToken PRO (Java) для использования в PKI-системах, а также может работать без подключения к компьютеру как автономный генератор одноразовых паролей.

Одноразовый пароль может быть использован для:

- аутентификации пользователей при удаленном VPN-доступе, доступе к Web-серверам, опубликованным Web-приложениям;
- подтверждения платежных операций.

Рекомендуется:

- сотрудникам организаций, которым требуется постоянный удаленный доступ к информационным ресурсам вне зависимости от типа используемого для выхода в Интернет устройства;
- банкам, кредитно-финансовым организациям – для повышения уровня доступности предоставляемых ими сервисов, повышения удовлетворенности клиентов качеством обслуживания;
- разработчикам систем ДБО – для создания конкурентоспособных систем ДБО, позволяющих банкам, использующим эти системы, повышать уровень доступности предоставляемых услуг.

eToken ГОСТ (сертификат ФСБ России)

eToken ГОСТ – персональное средство криптографической защиты информации для формирования электронной подписи по ГОСТ Р 34.10-2001 с неизвлекаемым закрытым ключом, выполненное в виде USB-ключа или смарт-карты. Использование eToken ГОСТ в составе существующих и разрабатываемых информационных систем повышает их защищенность и обеспечивает соответствие требованиям российского законодательства в части защиты информации.

Рекомендуется:

- разработчикам систем ДБО, электронных торговых площадок, систем сдачи налоговой отчетности – для обеспечения безопасности закрытых ключей электронной подписи пользователей этих систем;
- разработчикам СКЗИ – для использования в своих СКЗИ аппаратно реализованных российских криптографических алгоритмов, генератора ПСЧ, а также обеспечения неизвлекаемого хранения закрытых ключей;
- разработчикам СЗИ – для встраивания СКЗИ eToken ГОСТ в создаваемые ими продукты.

eToken ГОСТ имеет сертификат ФСБ России по классам защиты КС1 и КС2 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.

КриптоПро eToken CSP

КриптоПро eToken CSP – аппаратно-программное средство формирования квалифицированной электронной подписи с неизвлекаемым закрытым ключом. Данное решение обеспечивает полный набор криптографических операций, реализованных в СКЗИ КриптоПро CSP 3.6 и полную интеграцию с инфраструктурой PKI на базе КриптоПро УЦ. При этом все операции с закрытыми ключами электронной подписи выполняются аппаратно, а сами закрытые ключи никогда не покидают устройство и не могут быть перехвачены.

СКЗИ КриптоПро eToken CSP рекомендуется для использования в:

- автоматизированных системах органов государственной власти и местного самоуправления;
- системах защищенного юридически значимого электронного документооборота – для аутентификации пользователей и формирования электронной подписи;
- системах клиент-банк, электронных торгов – для подтверждения платежных операций;
- проектах с социальной / идентификационной картой;
- системах мобильных платежей.