eToken® TMS

система управления жизненным циклом
смарт-карт и USB-ключей

Краткая справочная информация

для специалистов
по информационной
безопасности и ИТ

Версия 1.2

В данном документе в краткой табличной форме приведена основная справочная информация по системе управления жизненным циклом смарт-карт и электронных USB-ключей eToken производства компании Aladdin.

Aladdin®
SECURITY SOLUTIONS
www.aladdin.ru

Краткая информация о продукте

Параметр	Краткое описание
eToken TMS	**eToken TMS** (Token Management System) - система, предназначенная для внедрения, управления, использования и учета аппаратных средств аутентификации пользователей (USB-ключей и смарт-карт eToken и др.) в масштабах предприятия. eToken TMS является связующим звеном между пользователями, средствами аутентификации, приложениями ИБ[1] и политикой безопасности (организационными правилами). eToken – это смарт-карта или электронный ключ, подключаемый к USB порту, предназначенный для строгой двухфакторной аутентификации пользователей при доступе к защищенным информационным ресурсам, для безопасного хранения ключевой информации, профилей пользователей и других конфиденциальных данных, для аппаратного выполнения криптографических вычислений и работы с асимметричными ключами и сертификатами X.509.
Основные модели используемых ключей	**eToken PRO**[2] (USB-ключ) **eToken PRO / SC** (смарт-карта) **eToken NG – OTP** (USB-ключ с системой OTP)
Фото	 eToken PRO (USB / смарт-карта)  eToken NG – OTP (USB-ключ с системой OTP)
Время появления продукта на рынке	◆ **Декабрь 2003 г.** – eToken TMS v.1.0 - первая версия продукта для управления жизненным циклом смарт-карт и упрощения использования технологий смарт-карт и PKI-решений, внедряемых на предприятиях. ◆ **Февраль 2005 г.** – eToken TMS v.1.1 - обновленная версия системы, выпущенная с учетом пожеланий и рекомендаций пользователей продукта. В эту версию добавлен комплект для разработки собственных модулей сопряжения - TMS Connector SDK, что позволяет расширять возможности системы и дорабатывать необходимые компоненты.
Используемые технологии	HTTP, HTTPS, LDAP (MS AD), PKCS #10, PKCS #11, PKCS #12, SSL, X.509 (MS CA), XML.
Ресурс для получения подробной актуальной информации	www.aladdin.ru etoken@aladdin.ru

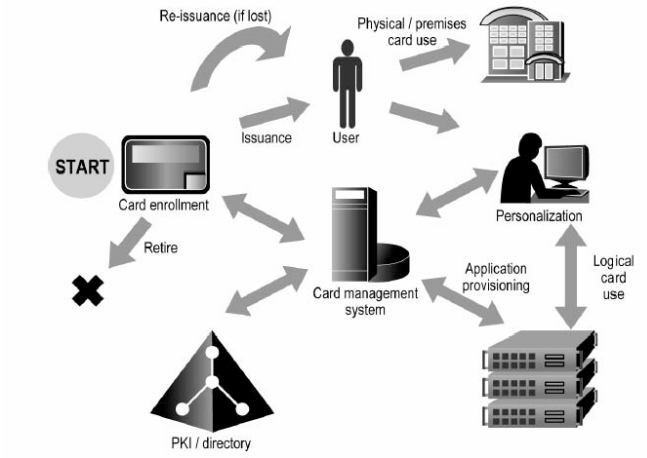
[1] ИБ – информационная безопасность

[2] В том числе и сертифицированные модели eToken PRO cert

Основное назначение и преимущества продукта

Назначение

- **Система TMS предназначена** для внедрения, управления, использования и учета средств аутентификации пользователей в масштабах организации. TMS - связующее звено между пользователями, средствами аутентификации, приложениями ИБ и политикой безопасности (организационными правилами).
- **Управление средствами аутентификации.** В системе допускается, что один пользователь может владеть одним или несколькими USB-ключами и/или смарт-картами.
- **Управление жизненным циклом** средств аутентификации и пользовательских данных состоит из следующих основных этапов:
  - выпуск смарт-карты или токена (далее "карты") для организации;
  - выдача карты сотруднику организации;
  - персонализация карты;
  - обслуживание карты:
    - добавление возможности доступа к новым приложениям;
    - отзыв предоставленного ранее доступа;
    - разблокирование PIN-кода;
  - замена / временная выдача новой карты;
  - отзыв карты.



Источник: Burton Group, август 2004

Возможности применения

- **eToken TMS позволяет** с минимальными затратами времени и средств выполнять основные задания по комплексному управлению USB-ключами и смарт-картами пользователей, в том числе:
  - создавать, импортировать, экспортировать, редактировать учётные записи пользователей;
  - назначать пользователям смарт-карты и USB-ключи;
  - записывать в памяти этих устройств сертификаты открытого ключа и закрытые ключи;
  - печатать фотографию, имя пользователя, штрих-код и другую информацию на комбинированных картах;
  - регистрировать имплантированные в карты радио-метки (RFID);
  - обновлять, отзывать сертификаты;
  - разблокировать устройства;
  - управлять полномочиями пользователей.

Основные возможности

- **Система базируется** на существующей в организации службе каталога Active Directory и использует имеющиеся в ней данные (например, о персонале).
- **Установка программного обеспечения.** eToken TMS совместим с основными системами развёртывания программного обеспечения.

	▪ **Web-интерфейс.** Пользователь работает с порталом через Web-интерфейс. Такой интерфейс служит для поддержки конечных пользователей и осуществления основных операций с токенами. Пользователь обращается в «стол справок» (Help Desk) по телефону или заходит на веб-сайт TMS и сообщает о возникновении проблемы. ▪ **Графический интерфейс TMS** представляет собой оснастки консоли управления Microsoft. Графический интерфейс TMS — это набор изолированных оснасток, расширений и двухрежимных оснасток (dual-mode snap-ins). Графический интерфейс TMS тесно интегрирован в существующие средства администрирования Microsoft, что является наиболее удобным для системного администратора. ▪ **Для работы с внешними приложениями** существуют набор программных компонентов – коннекторов. Текущая версия eToken TMS имеет в своем составе набор готовых коннекторов, позволяющих работать со следующими приложениями: ▪ Microsoft GINA (Network Logon (Gina) Connector); ▪ Microsoft CA (Microsoft CA Connector); ▪ Импорт сертификата с закрытым ключом (P12 Importing Tool Connector); ▪ Entrust CA (Entrust CA Connector). ▪ **Открытая архитектура**. Разработчики приложений могут использовать предлагаемый SDK для создания коннекторов TMS, что позволяет более гибко развивать систему под конкретные требования проекта и заказчика. Средство разработки коннекторов – TMS Connector SDK – входит в eToken TMS v.1.1. ▪ **Отчёты и аудит.** Информация обо всех действиях сохраняется в базе данных. При этом TMS может формировать отчёты: ▪ о том, какие пользователи имеют доступ к определённому приложению; ▪ о том, какие пользователи, в течение какого промежутка времени проходили удалённую регистрацию; ▪ о том, каким пользователям следует обновить свои токены.
Основные преимущества	▪ **Удобство и безопасность** ▪ Большинство операций по администрированию и сопровождению системы производится через браузер. Для поддержки конечных пользователей и осуществления ими основных операций с USB-ключами и смарт-картами служит веб-сайт. ▪ Управление и работа с TMS производится через удобный графический интерфейс. Графический интерфейс для администратора — это оснастки MMC консоли, основного средства администрирования Windows. Графический интерфейс пользователя — веб-интерфейс. ▪ На клиенте устанавливается только драйвер ключа eToken (RTE). В дополнительном программном обеспечении или специальном клиенте необходимости нет. ▪ Развёртывание программного обеспечения не является сложной задачей. TMS совместим с основными системами развёртывания программного обеспечения. Поддерживаются современные серверные платформы, на которые может быть установлен eToken TMS. ▪ **Интеграция с PKI решениями и MS Active Directory** ▪ Система обеспечивает централизованное издание сертификатов и управление правами пользователей в рамках всего предприятия. Цифровые сертификаты могут издаваться как средствами MS CA, так и внешними CA, например: Entrust CA, RSA Keon, VeriSign. ▪ Полная интеграция в Active Directory. Сегодня служба каталога MS Active Directory имеет широкое распространение и является лучшим решением для тех, кто его уже использует. Active Directory содержит надёжный механизм безопасности, поддерживает автоматическую репликацию между сайтами, позволяет импортировать пользователей из других систем. ▪ **Система eToken TMS ориентирована на использование USB-ключей и смарт-карт eToken**. Основное назначение этих ключей и смарт-карт – аутентификация пользователей и безопасное хранение закрытых ключей и сертификатов. Помимо этого eToken обеспечивает: ▪ Строгую аутентификацию пользователей за счет использования криптографических методов. ▪ Безопасное хранение закрытых ключей цифровых сертификатов для доступа к защищенным корпоративным сетям, информационным ресурсам, ключей для

	шифрования полей БД. ▪ Безопасное использование – воспользоваться ключом eToken может только его владелец, знающий PIN-код авторизации. ▪ Удобство работы – ключ выполнен в виде брелка со световой индикацией режимов работы и напрямую подключается к USB-портам, которыми сейчас оснащено 100% компьютеров, не требует специальных считывателей, блоков питания, проводов и т.п. ▪ Использование одного ключа для решения множества различных задач – входа в компьютер, входа в сеть, защиты канала, шифрования информации, ЭЦП, безопасного доступа к защищенным разделам Web-сайтов, информационных порталов и т.п.
Основной эффект, достигаемый от использования решения	▪ **Экономический эффект.** Уменьшение расходов на сопровождение путём автоматизации типовых операций: снятие блокировки PIN-кода, обновление сертификатов в режиме самообслуживания через веб-интерфейс и т.п. Внедрение системы eToken TMS позволяет снизить совокупную стоимость владения информационной системой (TCO) и увеличить возврат на инвестиции (ROI). ▪ **Технологический эффект.** Существенное повышение корпоративной безопасности благодаря использованию сертификатов открытого ключа стандарта X.509 и хранения закрытых ключей в защищённой памяти смарт-карт и USB-ключей. Внедрение системы eToken TMS повышает безопасность и управляемость IT-систем предприятия, переводит административный контроль и аудит на качественно новый уровень. ▪ **Эксплуатационный эффект** ▪ Внедренная система eToken TMS позволяет решать вопросы управления жизненным циклом USB-ключей и смарт-карт, что упрощает внедрение и управление на всех этапах использования этих устройств, а так же решает вопросы инвентаризации. ▪ Упрощение внедрения и эксплуатации PKI-решений с использованием USB-ключей и смарт-карт благодаря автоматизации типовых процедур администрирования и аудита IT-системы в целом.
Основные потребители	▪ **Крупные и средние компании**, использующие либо планирующие внедрение PKI-решений с использованием смарт-карт или USB-ключей eToken, и обрабатывающие критически важные для их бизнеса данные, пользующиеся системой электронного документооборота. ▪ **Органы государственной власти** и местного самоуправления, организации различных форм собственности, **работающие с конфиденциальной информацией** (в том числе с персональными данными граждан).
Возможность использования решения в гос. структурах	▪ **Компания Aladdin имеет все необходимые лицензии** ▪ Гостехкомиссии (ФСТЭК) РФ и ФАПСИ (ФСБ) на деятельность в области разработки, производства, услуг, распространения средств защиты и защищенных систем. ▪ Минэкономразвития на импорт шифровальных средств (eToken) и разрешение ФСБ на ввоз их на территорию России[3]. ▪ eToken TMS поддерживает **сертифицированные** электронные ключи и смарт-карты eToken PRO, имеющие сертификат № 925 Гостехкомиссии РФ (для защиты конфиденциальной информации и использования в АС до класса "1Г").
Простота внедрения, адаптация персонала	▪ **Для пользователей** – типовые рабочие действия с USB-ключами или смарт-картами интуитивно понятны (как с USB-flash диском) – подключил, ввел PIN-код и работай, не надо запоминать имена пользователей и пароли, имена серверов и пр. 

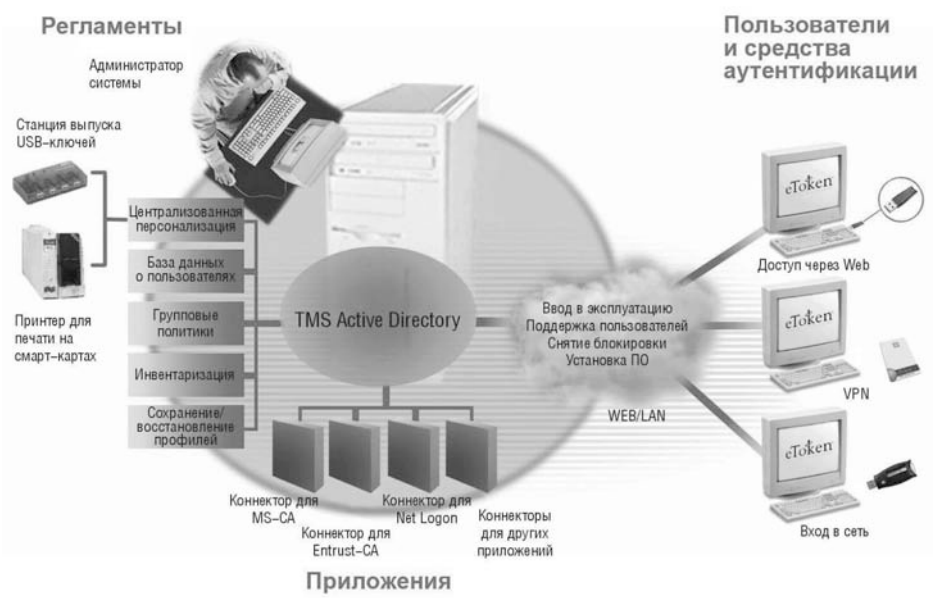
[3] Другие компании, осуществляющие ввоз подобных устройств на территорию России, таких разрешений и лицензий не имеют.

	Все служебные действия выполняются администратором системы или самим пользователем самостоятельно через веб-сайт. Такой подход не требует дополнительного обучения пользователей системы и снижает влияние "человеческого фактора" – риск некорректных действий пользователя минимален. ▪ **Для администраторов** – дистанционная установка клиентского ПО, использование групповых политик и пр. привычные инструменты администрирования. Графический интерфейс TMS тесно интегрирован в существующие средства администрирования Microsoft, что является наиболее удобным для системного администратора. Графический интерфейс для администратора — это оснастки MS MMC (MS MMC – основной интерфейс MS при выполнении административных функций на серверах MS Windows 2000/2003). К продукту eToken TMS прилагаются подробные инструкции и документация по настройке системы безопасности на русском и английском языках. ▪ **Для сотрудников службы безопасности** – использование централизованного управления, мониторинга и аудита изначально заложено в систему. Вся информация обо всех действиях сохраняется в центральной базе данных. eToken TMS может формировать отчёты: ▪ о том, какие пользователи имеют доступ к определённому приложению; ▪ о том, какие пользователи, в течение какого промежутка времени производили удалённую регистрацию; ▪ о том, каким пользователям следует обновить свои сертификаты. Управление может быть построено через графический интерфейс, тесно интегрированный в существующие средства администрирования Microsoft, либо через веб-сайт. ▪ **Для сотрудников служб тех. поддержки** – возможность самообслуживания пользователей через Help Desk с веб-интерфейсом (если пользователь забыл PIN, истек срок действия сертификата, необходимо получить доступ к новым приложениям или данным и т.п.).
Внедрение и сопровождение решения	Внедрение и сопровождение продукта и решений с его использованием (прикладных систем) может осуществляться партнерами компании Aladdin. Период гарантийного обслуживания - 3 месяца, платная программа обновлений версий и компонентов продукта (более подробно см. прайс-лист).
Системные требования	**Сервер:** ▪ Сервер Microsoft Windows Server 2000 SP3 с установленными компонентами .NET или ▪ Сервер Microsoft Windows 2003 Server. **Перед установкой** на сервере должна быть установлена и настроена служба каталога MS Active Directory. **На клиентских рабочих местах:** ▪ Операционная система Windows 9x/NT/2000/XP (рекомендуется XP Professional), Windows XP Embedded (для терминальных станций). ▪ Драйвер eToken RTE (версия 3.60 и выше). **На административном рабочем месте:** ▪ Операционная система Windows XP Professional SP2. ▪ Драйвер eToken RTE версии 3.60 (необходима версия 3.60 для запуска TMS Administrative Tools).

Технические подробности

1. Архитектура eToken TMS

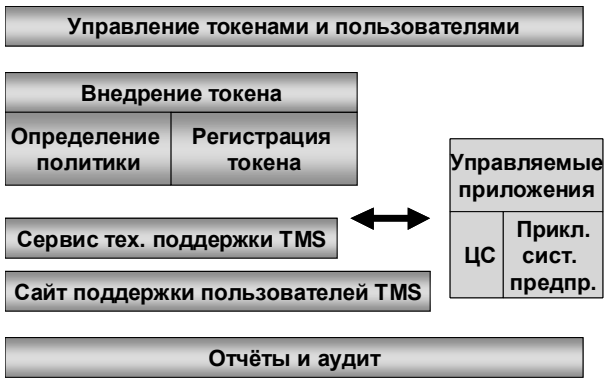
Инфраструктура TMS



Система eToken TMS предназначена для внедрения, управления и использования средств аутентификации пользователей в масштабах предприятия.

eToken TMS - связующее звено между пользователями, средствами аутентификации, приложениями и регламентами (политикой информационной безопасности, организационными правилами). eToken TMS предоставляет возможность управления eToken и другими средствами аутентификации в масштабах предприятия.

Основные компоненты



Краткое описание основных компонентов

Управление токенами и пользователями

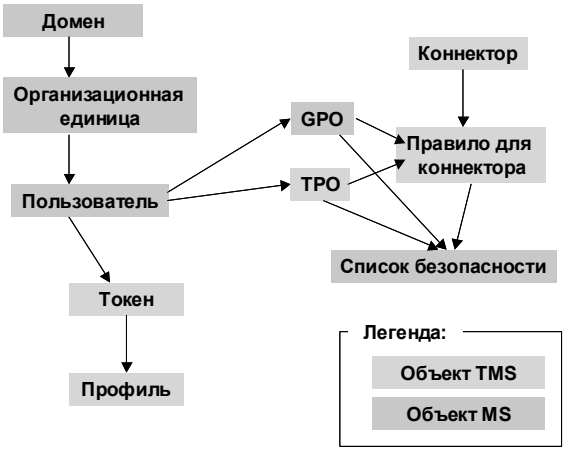
- Назначение токенов пользователям.
- Идентификация токенов и пользователей.
- Обработка ситуаций, возникающих в случае потери токенов.
- Отзыв токенов.
- Поддержка нескольких токенов для одного пользователя.
- Подпись токенов корпоративной подписью.

Внедрение токена

- **Определение политики.** Определение взаимной привязки приложений (с помощью организационных единиц AD (Active Directory), объектов групповой политики и объектов политики токенов (TPO, Token Policy Object)).
- **Регистрация токена**

	▪ **Локальная регистрация.** Администратор подготавливает токены для пользователей. Подготовка нескольких токенов одновременно с помощью концентратора USB. ▪ **Удалённая регистрация.** Пользователи загружают необходимое содержимое в токен с веб-сайта TMS, во время входа в систему или с помощью специального клиентского приложения для регистрации. Обновление содержимого токенов по необходимости. **Сервис технической поддержки TMS** ▪ TMS предоставляет готовое к использованию веб-приложение, используемое системными администраторами. **Сайт поддержки пользователей TMS** ▪ Веб-сайт для поддержки конечных пользователей и осуществления основных операций с токенами. **Управляемые приложения** ▪ **Регистрация токена** ▪ TMS взаимодействует с управляемыми приложениями и контролирует их с помощью коннекторов TMS. ▪ Коннекторы TMS используются при определении политики и регистрации токена. ▪ В настоящее время поддерживаются такие управляемые приложения, как Microsoft CA, Entrust CA*, Baltimore CA*, Verisign*, eToken Network Logon и другие. ▪ **Развёртывание программного обеспечения** ▪ TMS совместим с основными системами развёртывания программного обеспечения. ▪ Автоматическая установка и обновление различных клиентов безопасности (таких как RTE, GINA, VPN, Entrust client) на клиентских ПК осуществляется через локальную сеть предприятия. **Отчёты и аудит в TMS** ▪ Информация обо всех действиях сохраняется в центральной базе данных. TMS может формировать отчёты: ▪ о том, какие пользователи имеют доступ к определённому приложению; ▪ о том, какие пользователи, в течение какого промежутка времени осуществили удалённую регистрацию; ▪ о том, каким пользователям следует обновить свои данные на токенах (например, выписать новый сертификат для входа в сеть).
Потоки данных в TMS	 ▪ Графический интерфейс администратора — это оснастки MMC. ▪ Графический интерфейс пользователя — веб-интерфейс. ▪ Веб-регистрация работает на MS IIS. ▪ Открытая архитектура: разработчики приложений могут использовать TMS SDK для создания коннекторов TMS для своих приложений или для развития системы.

Системные объекты TMS



Терминология AD

- **Организационная единица** (Organization unit, OU) – особый тип группы пользователей AD. Пользователь может быть отнесён только к одной OU.
- **Объект групповой политики** (Group Policy Object, GPO) – группа политик, определяющих различные параметры пользователей и компьютеров. Обычно GPO назначается одной или нескольким OU.

Терминология TMS

- **Коннектор TMS**– набор программных компонентов, позволяющих TMS управлять определённым приложением.
- **Приложение TMS** – любое приложение, использующее eToken или другое устройство, совместимое с TMS при наличии соответствующего коннектора TMS.
- **TPO** (Token Policy Object, объект политики токенов) – объект AD, содержащий набор правил для коннекторов.

- **Правило TMS для коннектора** – правило, определяющее способ применения определённого приложения к группе пользователей в процессе регистрации.
- **Профиль токена TMS** – набор файлов, записываемых в eToken в процессе регистрации коннектором одного приложения для последующего использования этим приложением.
- **Виртуальный профиль TMS** – копия профиля токена TMS, сохранённая в AD.

2. Сценарии использования TMS

Порядок работы с TMS	**Установка** ▪ Установка TMS на сервере Active Directory. ▪ Установка одного или нескольких коннекторов TMS. **Назначение регистрации** ▪ Назначение организационной единице одного или нескольких правил для коннекторов TMS. **Процесс регистрации может осуществляться по одному из следующих путей:** ▪ Администратор может осуществлять локальную регистрацию для пользовательских токенов. ▪ Администратор может отправлять по электронной почте сообщение группе пользователей с просьбой осуществить веб-регистрацию. ▪ Пользователь может осуществить веб-регистрацию, зайдя на сервер веб-регистрации TMS и следуя инструкциям на этом сервере. ▪ Процесс регистрации может происходить автоматически при входе пользователей в систему. **Управление токенами** ▪ Добавление токена в базу данных TMS. ▪ Назначение пользователям токенов. ▪ Нахождение пользователя, являющегося владельцем токена. ▪ Отзыв токена.
Пользователь забыл PIN-код	1. **Сообщение о возникновении проблемы.** Пользователь может воспользоваться «справочным столом» (службой Help Desk), сообщить о возникновении проблемы и получить одноразовый пароль, либо сообщить о проблеме на веб-сайте TMS. Одноразовый пароль сообщается по телефону, SMS, электронной почте и т. д. 2. **Аутентификация и вход в систему.** Пользователь входит в систему удалённой поддержки TMS с помощью одноразового пароля. В качестве альтернативы, одноразовый пароль может быть использован для входа в Windows (только один раз). 3. **Идентификация eToken.** Пользователя просят подключить свой eToken к порту USB. После этого система пытается разблокировать eToken с помощью пароля администратора eToken. 4. **Смена PIN-кода.** Пользователь вводит новый PIN-код.
Пользователь потерял eToken	1. Пользователь обращается в «стол справок» по телефону или заходит на веб-сайт TMS и сообщает о возникновении проблемы. 2. Администратор находит пользователя в базе данных и определяет eToken, который принадлежит данному пользователю. 3. Администратор выделяет eToken и запускает процесс “потерянный eToken”. 4. TMS просит администратора ввести новый eToken (для замены потерянного). 5. TMS копирует все идентификационные данные, из архивов в новый eToken. 6. TMS отзывает все идентификационные данные, у которых не было резервных копий, но которые присутствовали в старом eToken, из ЦС и других систем. 7. TMS создаёт недостающие идентификационные данные и сертификаты на новом eToken.
Пользователь забыл eToken дома, и ему нужно сегодня работать	Этот сценарий аналогичен процессу “потерянный eToken”, но старый eToken не отзывается, а блокируется. 1. Пользователь обращается в «стол справок». 2. Администратор находит пользователя в базе данных и запускает процесс “Временный eToken”. 3. TMS готовит для пользователя временный eToken. 4. TMS настраивает временный eToken таким образом, что он автоматически станет недействительным на следующий день. 5. Для того чтобы разблокировать свой обычный eToken, пользователь должен вернуть временный eToken в «стол справок».
Пользователь покидает компанию	1. Пользователь возвращает свой eToken в «стол справок». 2. Администратор отзывает eToken и переформатирует его.

3. eToken – надежность, безопасность, совместимость

Сертификаты безопасности	Рекомендуемая модель ключа/смарт-карты для использования с eToken TMS - eToken PRO. Сертификаты безопасности на eToken PRO: ▪ Сертификат №925 Гостехкомиссии РФ (для защиты конфиденциальной информации и использования в АС до класса "1Г" вкл.) ▪ 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 4/5 ▪ 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)
Дипломы и награды eToken	▪ "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, ж-л "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, ж-л "Бизнес и безопасность в России") ▪ "За достижения в индустрии безопасности" - диплом (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 (на eToken)	▪ Microsoft (Designed for Windows XP) ▪ Cisco (Cisco Systems Verified, Cisco AVVID Partner) ▪ Computer Associates (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) ▪ Baltimore (PKIWorld partner program, Technology Partner) ▪ VeriSign
Мобильность и удобство использования	
Необходимость перезагрузки рабочей станции после инсталляции (для Windows XP, 2000)	Не требуется
Необходимость использования дополнительных устройств считывания для подключения eToken к компьютеру	USB-ключи eToken PRO и NG – OTP напрямую подключаются к USB-порту, дополнительных считывателей не требуется. При использовании смарт-карт eToken PRO требуется любой PC/SC совместимый карт-ридер, например, ASEdrive, поставляемый компанией Aladdin.

Инфраструктура	
Техническая поддержка от производителя / поставщика на русском языке	Есть.
Наличие необходимых лицензий у поставщика, разрешений на экспорт/импорт идентификаторов	Aladdin имеет все необходимые лицензии Гостехкомиссии РФ и ФАПСИ на деятельность в области разработки, производства, услуг, распространения средств защиты и защищенных систем (не вкл. гостайну), а также необходимые разрешения ФСБ на ввоз/вывоз eToken.
Наличие интеграторов, имеющих опыт и специалистов по внедрению решения	Внедрение и сопровождение продукта и решений с его использованием (прикладных систем) может осуществляться партнерами компании Aladdin.

Пример внедрения

Муниципалитет Herning, Дания	
Общие сведения и постановка задачи	**Общие сведения** ▪ 58,300 жителей. ▪ ЭЦП и шифрование документов. **Постановка задачи** ▪ ЭЦП и шифрование документов согласно требованиям датского законодательства. ▪ Усиленная безопасность с применением двухфакторной аутентификации. ▪ Передача документов по VPN-каналу. ▪ Обеспечение безопасных электронных транзакций. ▪ Интеграция со СКУД[4].
Этапы проекта	**Начальный этап** ▪ 1200 eToken PRO/32K для работников муниципалитета. ▪ TMS + коннектор для Microsoft CA. ▪ Строгая аутентификация для CA eTrust SSO, и через него - в унаследованные приложения. **Развитие проекта** ▪ Интеграция со СКУД (RFID-метки - HID). ▪ Распространение решения для всех жителей города.
Ключевые факторы успеха	▪ Возможности TMS по управлению eToken. ▪ Поддержка eToken многими приложениями.
Итоги проекта	▪ **Успешное внедрение смарт-карт** для решения задач информационной безопасности при количестве рабочих мест более 100 практически невозможно без использования ПО управления жизненным циклом смарт-карт. ▪ **TMS - зрелая технология**, на практике доказывающая свою эффективность.

[4] СКУД – система контроля и управления доступом в помещения

Основные угрозы и методы противодействия им

В таблице (ниже) приведены основные угрозы и методы противодействия им, реализованные в продукте.

Угроза	Противодействие	Метод
Кража и использование данных чужой учетной записи (из-за отсутствия защиты учетной записи)	Аутентификация по цифровому сертификату.	Использование механизма SSL аутентификации.
Использование известных паролей, установленных по умолчанию (если он не был переустановлен пользователем)	Аутентификация по цифровому сертификату.	Отказ от использования паролей, переход на SSL аутентификацию с использованием сертификатов.
Кража пароля (например, с использованием снифера - ПО для перехвата вводимых паролей)		
Подбор пароля (например, методом перебора по словарю)		
Перехват пароля во время передачи по сети		
Кража или копирование ключевого контейнера или его резервной копии	Закрытый ключ хранится как не экспортируемый в защищенной памяти смарт-карты или USB-ключа eToken.	Использование смарт-карт технологий для безопасного хранения закрытых ключей.
Перехват закрытого ключа (в момент его использования с помощью специального ПО)	Аппаратная реализация криптографических операций в смарт-карте или USB-ключе eToken PRO.	Использование смарт-карт технологий для аппаратного выполнения криптографических операций (SSL) в процессоре карты без "выхода" закрытых ключей наружу.
Кража eToken	Доступ к защищенной памяти eToken, в которой хранятся закрытые ключи, защищен PIN-кодом.	В eToken реализован контроль длины и качества задаваемого пользователем PIN-кода и запрет использования "слабых" комбинаций (может задаваться в групповых политиках). При форматировании eToken PRO имеется возможность задания количества неправильно введенных подряд PIN-кодов (пользователя и/или администратора), после чего eToken блокируется.
Подбор PIN-кода eToken	Задание уровня сложности вводимых пользователями PIN-кодов и блокирование eToken после N подряд введенных неправильных значений.	
Дублирование eToken (копирование закрытых ключей в другой токен)	Доступ к защищенной памяти eToken, в которой хранятся закрытые ключи, защищен PIN-кодом. Закрытые ключи не могут быть экспортированы из eToken PRO.	Закрытые ключи, сгенерированные eToken или импортированные в него, хранятся в закрытой памяти смарт-карты и не могут быть из нее извлечены. Это подтверждается международными сертификатами безопасности ITSEC Level E4, FIPS 140-1 – Level 2, 3.
Перехват трафика между ключом eToken и компьютером	Защищенный обмен данными.	В eToken предусмотрена возможность шифрования трафика с использованием Secure Messaging по алгоритму 3DES (CBC).
Перехват передаваемых по сети данных	Шифрование сетевого трафика.	Использование SSL протокола для шифрования передаваемых по сети данных.

Aladdin
SECURITY SOLUTIONS

101000, Москва, Милютинский пер., 14.
Тел: (095) 231-3113
E-mail: aladdin@aladdin.ru
Web: www.aladdin.ru

Лицензии Гостехкомиссии России №№ 0037, 0054 от 18.02.03
Лицензии ФАПСИ №№ ЛФ/07-2635-38 от 24.04.02
Microsoft Certified Partner, IBM Business Partner, Oracle Business Partner