Централизованная система учета, ввода в эксплуатацию, управления и аудита использования всех средств аутентификации и хранения ключевой информации, используемых на предприятии

Технические спецификации

Операционная система на стороне сервера	Microsoft Windows Server 2000 и 2003
Операционная система на стороне клиента	Microsoft Windows Vista, XP, 2000, Linux, Mac OS (для USB-ключей и смарт-карт). Любые типы ОС (для eToken PASS и eToken NG-OTP в режиме генератора одноразовых паролей).
Устройства eToken	Все типы и модели электронных ключей eToken: • USB-ключ eToken PRO • Смарт-карта eToken PRO • Комбинированный USB-ключ eToken NG-OTP • Комбинированный USB-ключ eToken NG-FLASH • Генератор одноразовых паролей eToken PASS • USB-ключи и смарт-карты eToken со встроенными бесконтактными радио-метками (RFID) • Виртуальный токен
Службы каталога (базы учетных данных пользователей)	• Microsoft Active Directory • OpenLDAP • Microsoft SQL Server
Конфигурации Microsoft Active Directory	• Основной домен (Production Domain) • Теневой домен (Shadow Domain) • Режим приложений Active Directory (ADAM, Active Directory Application Mode)
Конфигурации без использования Microsoft Active Directory	• Microsoft SQL Server + ADAM • OpenLDAP + ADAM
Поддерживаемые приложения и аппаратные устройства	• Центры сертификации: Microsoft CA, RSA Keon, Крипто-Про УЦ • Клиентское ПО виртуальных частных сетей - Check Point VPN, Microsoft VPN, Cisco VPN и др. • ПО для двухфакторной аутентификации пользователей на серверах и рабочих станциях Windows - eToken Windows Logon • ПО для двухфакторной аутентификации пользователей при доступе к различным приложениям Windows – eToken Simple Sign-On • Система защиты конфиденциальной информации и персональных данных для Windows XP/2000 – Secret Disk • Устройства Cisco ISR (Integrated Services Routers), Cisco ASA
Поддержка других приложений или аппаратных устройств	Через механизм интерфейсных программных модулей (коннекторов), для написания которых предлагается специальный комплект разработчика eToken TMS 2.0 Connector SDK
Поддержка русского языка	Да

ID: M01301-0508

Aladdin SECURITY SOLUTIONS

© 2008, Aladdin Software Security R.D.
Тел.: (495) 223-0001
E-mail: aladdin@aladdin.ru
Web: www.aladdin.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (продлены до 18.02.13)
Лицензии ФСБ России № 2683Р от 02.09.05, №№ 4205П, 4206Х, 4207Р от 22.06.07 и № 4898П от 14.12.07
Microsoft Certified Partner, IBM Business Partner, Oracle Business Partner

eToken® TMS Token Management System

Централизованная система учета, ввода в эксплуатацию, управления и аудита использования всех средств аутентификации и хранения ключевой информации, используемых на предприятии

- Поэкземплярный учет и регистрация ключей eToken
- Ускорение ввода ключей в эксплуатацию
- Управление жизненным циклом ключей eToken
- Аудит использования ключей eToken
- Подготовка отчетов
- Техническая поддержка пользователей

Aladdin® SECURITY SOLUTIONS

Назначение

- **Поэкземплярный учет и регистрация** всех аппаратных и программных средств аутентификации и хранения ключевой информации, используемых сотрудниками.
- **Ускорение ввода в эксплуатацию** электронных ключей и смарт-карт, автоматизация процессов выдачи eToken сотруднику, персонализации eToken, записи ключевой информации и аутентификационных данных в память eToken.
- **Управление жизненным циклом** средств аутентификации и хранения ключевой информации: обновление аутентификационных данных и ключевой информации, предоставление / отзыв прав доступа к приложениям при изменении служебных обязанностей / увольнении сотрудника, замена устройства при его утере / повреждении, вывод устройства из эксплуатации.
- **Аудит использования** сотрудником выданного ему средства аутентификации и хранения ключевой информации (фиксируются все факты использования устройства сотрудником на компьютере предприятия, изменения хранящихся в памяти устройства данных).
- **Подготовка отчетов** для руководителей служб ИТ и ИБ об использовании сотрудниками средств аутентификации и хранения ключевой информации (на основе данных аудита средствами встроенного генератора отчетов, также имеется возможность экспорта данных во внешние средства построения отчетов).
- **Техническая поддержка** и сопровождение пользователей средств аутентификации через веб-сайт технической поддержки: переустановка забытого пользователем PIN-кода устройства, синхронизация генератора одноразовых паролей, обработка типовых ситуаций «пользователь забыл eToken», «пользователь потерял eToken», «пользователь повредил / сломал eToken».

Возможности

- Поддержка всех типов и моделей электронных ключей eToken.
- Интеграция со службой каталога Microsoft Active Directory, OpenLDAP, базой данных Microsoft SQL Server.
- Веб-сайты для самостоятельного решения пользователем проблем, возникающих в ходе эксплуатации eToken (user self-service web site), оказания технической поддержки пользователям eToken специалистом сервисной службы (help desk web site), веб-сайт для администрирования системы.
- Открытая архитектура, позволяющая добавлять в систему поддержку новых приложений и аппаратных устройств (через механизм коннекторов).
- Масштабируемое, распределенное администрирование:
  - администрирование систем eToken TMS, установленных в разных доменах, с одного рабочего места администратора;
  - ролевое администрирование, возможность делегирования полномочий.
- Аудит использования средств аутентификации и хранения ключевой информации сотрудниками, гибкая система построения отчетов на основе данных аудита.
- Отказоустойчивость и масштабируемость системы, поддержка кластерных технологий Microsoft Windows 2003.
- Централизованная установка клиентского ПО на рабочие станции пользователей.
- Широкий спектр поддерживаемых клиентских ОС: Windows, Linux, Mac OS; любая ОС при использовании одноразовых паролей.
- Полная поддержка русского языка.
- Виртуальный токен – уникальное программное решение, позволяющее пользователю, находящемуся вне офиса, даже в случае утери / повреждения eToken продолжить работу с компьютером или получить безопасный доступ к ресурсам без снижения уровня защищенности.

Когда необходим eToken TMS

- При внедрении на предприятии 100 и более eToken.
- При использовании схем аутентификации на основе одноразовых паролей (OTP - One Time Password) - например, для обеспечения безопасного удаленного доступа к информационным ресурсам с мобильных компьютеров, смартфонов и пр.
- При наличии сотрудников, работающих вне офиса или выезжающих в командировки.

eToken® eToken – персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭЦП. eToken выпускается в форм-факторах USB-ключа, смарт-карты или брелока. Модель eToken NG-OTP имеет встроенный генератор одноразовых паролей. Модель eToken NG-FLASH имеет встроенный модуль флэш-памяти объемом до 4 ГБ. Модель eToken PASS содержит только генератор одноразовых паролей. Дополнительно eToken могут иметь встроенные бесконтактные радио-метки (RFID-метки), что позволяет использовать eToken также и для доступа в помещения.

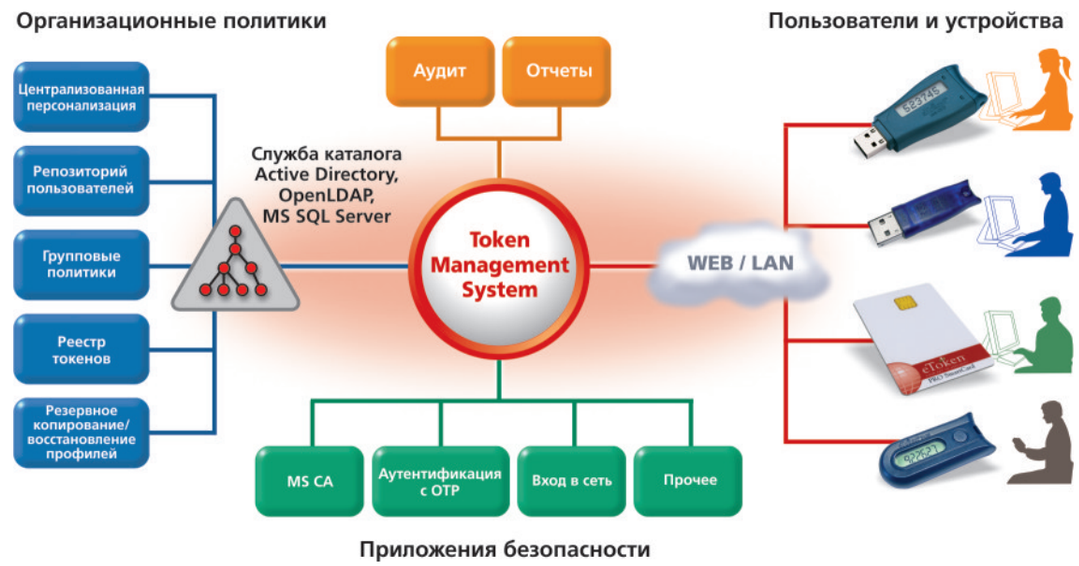
Модели eToken, сертифицированые ФСТЭК России, следует использовать для аутентификации пользователей и хранения ключевой информации в автоматизированных системах, обрабатывающих конфиденциальную информацию, до класса защищенности 1Г включительно. Они являются рекомендуемыми носителями ключевой информации для сертифицированных СКЗИ (КриптоПро CSP, Крипто-КОМ, Домен-К, Верба-OW и др.).

- Для приведения в соответствие автоматизированной системы предприятия требованиям законодательства, отраслевых и международных стандартов, других регламентирующих документов, в том числе:
  - ФЗ РФ «О персональных данных» от 27 июля 2006 года № 152-ФЗ
  - Руководящим документам Гостехкомиссии (ФСТЭК) России
  - Стандарту Банка России стандарта «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0–2006)
  - Международным стандартам HIPPA, Basel II, SOX и др.

Преимущества использования eToken TMS

- Высокая степень доступности информационных ресурсов предприятия, т.к. даже в случае утери / повреждения eToken доступ сотрудника может быть быстро восстановлен без снижения уровня защищенности информационной системы.
- Ведение единого реестра средств аутентификации и хранения ключевой информации, аудит их использования сотрудниками, контроль прав доступа сотрудников к отдельным приложениям, обеспечение безопасного доступа к информационным ресурсам.
- Снижение совокупной стоимости владения информационной системой. Внедрение eToken TMS позволит сократить потери времени сотрудников на ожидание получения доступа к информационным ресурсам.
- Уменьшение нагрузки на службы администрирования и поддержки, поскольку большинство типичных для конечного пользователя проблем могут быть разрешены самими пользователями через веб-сайт для самостоятельного решения проблем (user self-service web site).

Как работает eToken TMS



Отличительные особенности eToken TMS

- Единая система управления жизненным циклом для всех аппаратных и программных средств аутентификации и хранения ключевой информации, используемых сотрудниками, вне зависимости от их форм-фактора (USB-ключ или смарт-карта), реализуемого метода аутентификации (закрытые ключи и сертификаты, одноразовые пароли, хранимые в памяти учетные данные).
- Полная интеграция со службой каталога Microsoft Active Directory:
  - знакомые и интуитивно понятные администраторам средства администрирования и управления;
  - использование учетных данных пользователей, уже хранящихся в службе каталога – нет необходимости репликации данных;
  - использование механизмов групповой политики;
  - все пользовательские данные хранятся и обрабатываются в одном месте.
- Возможность использования в среде без Microsoft Active Directory.
- Используются только стандартные механизмы и протоколы аутентификации, поддерживаемые Microsoft Windows, не используются пропиетарные сервера аутентификации.
- Модульная архитектура - поддержка новых приложений и аппаратных устройств реализуется через механизм интерфейсных программных модулей (коннекторов), для написания которых предлагается специальный комплект разработчика eToken TMS 2.0 Connector SDK.