

Информационная безопасность:

ПРОДУКТЫ
РЕШЕНИЯ
ТЕХНОЛОГИИ



Token[™]

www.aladdin.ru
ALADDIN
SOFTWARE SECURITY R. D.

ALERO
SOFTWARE B.V.

Выпуск 1

Спонсор издания каталога: **Microsoft**

Настоящий каталог содержит описание продуктов и технологий, предназначенных для использования при построении современных систем информационной безопасности.

Представленные в каталоге решения:

- являются законченными решениями в области информационной безопасности;
- имеют открытый интерфейс;
- соответствуют принятым отраслевым и международным стандартам;
- позволяют использовать современные и универсальные аппаратные средства аутентификации приложений и пользователей, предоставляют возможность безопасного хранения ключевой информации в защищенной памяти ключей eToken.

Также в каталоге приведен ряд компаний, осуществляющих

- комплексные работы по проектированию, внедрению и сопровождению систем информационной безопасности;
- обучение и сертификацию специалистов в области информационной безопасности;
- издание и продвижение решений в области информационной безопасности;
- освещение вопросов, связанных с рынком систем информационной безопасности.

Издатели каталога надеются, что он будет выходить регулярно и сможет помочь владельцам и администраторам информационных систем сформировать комплексное видение ряда современных решений в области информационной безопасности и использовать эти решения в своих системах.



ВВЕДЕНИЕ	1
СОДЕРЖАНИЕ	2
ДОСТУП К СЕТЕВЫМ РЕСУРСАМ	3
■ eToken – безопасность в сети Windows 2000/XP	3
■ eToken для Lotus Notes	4
■ The Bat! Pro – защищенный почтовый клиент	5
■ Terminal AuthPro – аутентификация удаленных клиентов для MS Terminal Server и Citrix MetaFram	6
ДОСТУП К ИНТЕРНЕТ-РЕСУРСАМ	7
■ eToken Web Access Control – доступ к защищенным разделам Web-сайта	7
■ Город-Инфо – защищенный корпоративный портал	8
■ eToken Internet Logon – защищенный доступ к сети Интернет	9
ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN)	10
■ VPN «Застава»	10
■ VPN ViPNet	11
■ eToken для Check Point SecureRemote VPN-1	12
■ «ФПСУ-IP» – комплексы межсетевого экранирования	13
СИСТЕМЫ PKI	14
■ eToken для цифровых сертификатов VeriSign	14
■ eToken для HP Praesidium PKI (Baltimore UniCERT)	15
■ eToken для RSA Keon	16
ДОСТУП К КОРПОРАТИВНЫМ РЕСУРСАМ	17
■ eToken для защищенного доступа к системе управления предприятием SAP R/3	17
■ O'KEY 7.7 – аутентификация пользователей в системе «1С: Предприятие»	18
■ eToken для Documentum 4i	19
■ eToken для DOCS Open	20
■ eToken для CyberDOCS	21
■ Защищенная система управления распределенной сетью торговых предприятий	22
■ Matrix – защищенная система управления доступом к информации	23
ЗАЩИТА ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ	24
■ Электронный замок eToken PC-Lock	24
■ Crypton Lock – управление доступом к рабочим станциям	25
■ Secret Disk – система защиты конфиденциальной информации	26
ТЕХНОЛОГИИ	27
■ eToken – семейство электронных ключей	27
■ КриптоПро CSP – средство криптографической защиты	28
■ КриптоТраст – Центры Сертификации и Регистрации	29
■ Instant Obtain – система интернет-платежей	30
ВНЕДРЕНИЕ И СОПРОВОЖДЕНИЕ	31
■ «Кварта Технологии»	31
■ «Служба F1»	32
ОБУЧЕНИЕ И СЕРТИФИКАЦИЯ	33
■ Учебный Центр «ИНФОРМЗАЩИТА»	33
■ Авторизованный Учебный Центр «САМАН»	34
ИЗДАНИЕ, ПРОДВИЖЕНИЕ	35
■ ALERO Software Alliance B.V.	35
■ Проект InfoSecurity.ru – ресурс по информационной безопасности	36

eToken – безопасность в сети

USB-ключи для удобной и безопасной работы
в сети Windows 2000/XP

- Вход в сеть
- Хранение сертификатов
- Подпись и шифрование почты
- Автоматическое блокирование компьютера и/или отключение от сети при отсоединении ключа от USB-порта

Назначение

eToken позволит отказаться от использования паролей при входе в сеть и при защите конфиденциальной переписки. Пользователям не надо запоминать сложные пароли и периодически их менять – достаточно подключить электронный ключ eToken к USB-порту и ввести PIN-код. При этом значительно повышается защищенность сети и удобство работы.

Возможности

- Аппаратная двухфакторная аутентификация пользователя при входе в сеть (eToken вместо пароля).
- Блокирование компьютера и/или автоматическое отключение от сети при отсоединении eToken.
- Защита переписки для MS Outlook/Express (безопасное хранение сертификатов, защита от несанкционированного доступа, шифрование и цифровая подпись).
- Хранение цифровых сертификатов X.509 в защищенной памяти брелка eToken, а не на диске.
- Полная интеграция в Windows 2000/XP, поддержка PKI.
- Возможность использования одного eToken различными приложениями.
- Возможность использования сертифицированного ФАПСИ криптопровайдера CSP с длиной ключа 256 бит.

Эффективность защиты напрямую зависит от качества используемых паролей. Использование усиленной аутентификации с помощью eToken решает проблему подбора и перехвата паролей, особенно при удаленной работе в сети.

Продукт выпущен компанией Aladdin Software Security R.D. в рамках совместной программы с российским отделением Microsoft и фирмой «Крипто-Про».

Аладдин Р. Д.
(095) 231-31-13
security@aladdin.ru
www.aladdin.ru



eToken для Lotus Notes

Усиленная аутентификация пользователей при доступе к корпоративным базам Lotus Notes/Domino

- Повышение общего уровня безопасности системы
- Снижение риска утечки корпоративной информации
- Доступ к рабочему месту Lotus Notes с помощью ключа eToken
- Блокирование рабочего места Lotus Notes при отсоединении eToken

Назначение

Использование eToken для входа в Lotus Notes позволяет существенно повысить уровень защищенности и удобства работы с системой. Пользователям не нужно запоминать сложные пароли и периодически их менять – достаточно подключить электронный ключ eToken к USB-порту и ввести его PIN-код. Использование усиленной аутентификации с помощью eToken решает проблему подбора паролей и несанкционированного доступа к корпоративной информации посторонними лицами.

Возможности

- Доступ к рабочему месту Lotus Notes с помощью eToken.
- Блокирование рабочей станции и очистка сведений о пользователе при отсоединении электронного ключа.
- Хранение ID-файлов в защищенной памяти электронных ключей, а не на диске.
- Возможность использования сложного пароля для защиты рабочего места пользователя.
- Автоматический переход на работу с другим ID-файлом при отсоединении одного ключа eToken и подключении другого.
- Отказ от использования дискет для переноса ID-файла при работе на другом компьютере.

Чтобы работать со своим рабочим местом Lotus Notes на другом компьютере, пользователям не нужно каждый раз перезаписывать свой ID-файл с дискеты – достаточно подключить eToken к USB-порту и ввести его PIN-код.

Системные требования

Windows 9x, NT, 2000
Lotus Notes/Domino 4.6 – 6.0

Продукт выпущен в рамках совместного проекта компаниями «ИнтерТраст» и Aladdin Software Security R.D.



ИнтерТраст
(095) 956-79-28
(многоканальный)
intertrust@intrust.ru



Аладдин Р. Д.
(095) 231-31-13
security@aladdin.ru
www.aladdin.ru



The Bat! Pro – защищенный почтовый клиент

Знаменитая почтовая программа The Bat! в защищенном варианте

- Аппаратная аутентификация доступа к почтовым серверам
- Защита электронной почты, архива переписки и адресной книги
- Защищенные dial-up и почтовые ящики
- Невозможность перехвата паролей
- Поддержка цифровых сертификатов X.509
- Совместимость с MS Office
- Безопасный html-viewer

Назначение

The Bat! Pro – мощный и удобный защищенный клиент электронной почты со множеством уникальных функций. Он может использоваться как частными пользователями, так и корпоративными. The Bat! Pro имеет мощные средства фильтрации и обработки писем, диспетчер для манипуляций с письмами непосредственно на сервере.

The Bat! Pro – отличный инструмент для формирования запросов, подлежащих автоматической обработке, и эффективное средство управления электронным документооборотом.

Возможности

- Поддержка неограниченного числа почтовых ящиков на различных серверах.
- Независимая настройка каждого почтового ящика и одновременная работа с ними.
- Ведение журналов работы для каждого ящика.
- Мощные средства поиска и встроенные средства просмотра графических файлов.
- Автопроверка орфографии на нескольких языках.
- Встроенные функции почтового сервера локальной сети (TCP/IP – Non-TCP/IP шлюз).
- Мощные средства фильтрации писем.
- Встроенный Back-Up и функция дозвона.
- Шаблоны сообщений и «быстрые шаблоны», вставляющие заранее заготовленный текст, экономят много времени при написании писем.

Продукт выпущен в рамках совместного проекта компаниями RitLabs и Aladdin Software Security R.D.



RitLabs
+373-2-246889
office@ritlabs.com
www.ritlabs.com/ru/

Аладдин Р. Д.
(095) 231-3113 (30 линий)
aladdin@aladdin.ru
www.aladdin.ru



eToken Terminal AuthPro

Аутентификация удаленных клиентов для MS Terminal Server и Citrix MetaFrame при подключении к серверам на платформе Windows 2000/XP

- Усиленная аутентификация пользователей
- Хранение цифровых сертификатов в защищенной памяти eToken
- Блокирование удаленной сессии при отсоединении eToken на клиентском компьютере
- Доступ серверных приложений к клиентскому ключу

Назначение

- Аппаратная аутентификация удаленных клиентов с помощью USB-ключа eToken для решения проблемы подключения терминальных сессий под управлением MS Terminal Server и Citrix MetaFrame к серверам на платформе Windows 2000/XP.
- Предоставление серверным приложениям программного интерфейса для блокирования сессий и защищенного доступа к информации, хранящейся в памяти установленных на удаленном клиенте ключей eToken.

Возможности

- Удаленный вход в сеть с помощью eToken.
- Блокирование удаленной сессии при отсоединении электронного брелка eToken от клиентского компьютера.
- Хранение цифровых сертификатов и дополнительной информации для серверных приложений в защищенной памяти eToken, а не на диске.
- PIN-авторизация пользователей.
- Возможность использования одного eToken различными приложениями.
- Полная интеграция в Windows 2000/XP, поддержка PKI.

Вы всегда точно знаете, кто есть кто!

Продукт выпущен в рамках совместного проекта компаниями ExpertMark Labs и Aladdin Software Security R.D.



Эксперт Марк
(095) 218-7396
expert@expertmark.ru
www.expertmark.ru



Аладдин Р. Д.
(095) 231-3113
security@aladdin.ru
www.aladdin.ru

eToken Web Access Control

Аутентификация удаленных клиентов при доступе к защищенным разделам web-сайта

- Усиленная аутентификация пользователей
- Не требует привлечения провайдера и сложных настроек на сервере
- Может использоваться на виртуальных web-серверах

Назначение

eToken WAC предназначен для применения на виртуальных www-серверах, арендуемых у провайдера. eToken WAC прост и удобен в использовании, так как для применения необходимо лишь наличие на сервере CGI директории (возможность запускать на сервере программы, сценарии).

- Усиленная аутентификация для доступа к виртуальным www-серверам.
- Обеспечение безопасности при доступе к защищенным разделам web-сайта.
- Независимая от провайдера схема аутентификации.
- Гарантированная идентификация пользователей.

Возможности

- Быстрая установка и настройка.
- Требуется только исполняемая директория.
- Ведение собственной пользовательской базы.
- Автоматический выход из защищаемой области www-сервера при отсоединении ключа.
- Возможность удаленного перепрограммирования eToken.

eToken ActiveX позволяет разработчикам быстро добавлять в свои приложения усиленную аутентификацию по алгоритму DESX на основе протокола «запрос-ответ».

eToken WAC поставляется с инструкциями для разработчиков, сценариями на VB и примерами кода.

Платформы

Сервер: Windows NT/2000– IIS 4.0/5.0; BSD-based OS (FreeBSD, OpenBSD, BSDI)
Клиент: Windows 98Se/Me/NT/2000 с Internet Explorer 5.5 или выше.



Аладдин Р. Д.
(095) 231-3113 (30 линий)
aladdin@aladdin.ru
http://www.aladdin.ru



Защищенный корпоративный портал

– ядро информационной системы предприятия

- Эффективное управление информационными ресурсами предприятия
- Единый web-интерфейс для корпоративных пользователей
- Прозрачные схемы управления информацией
- Хранилище корпоративной информации
- Аутентификация пользователей при доступе к информационным ресурсам

Назначение

Корпоративный информационный портал – это программный продукт, обеспечивающий повышение эффективности корпоративного управления и взаимодействия сотрудников. Основные задачи продукта – создание единого интерфейса к структурированным и неструктурированным данным из различных источников, обеспечение групповой работы и обмен неформализованными корпоративными знаниями. Корпоративный информационный портал строится на базе web-технологий и позволяет интегрировать корпоративные приложения, используемые на предприятии: системы управления взаимоотношениями с клиентами (CRM), финансовые и бухгалтерские программы, специализированное программное обеспечение. С помощью корпоративного портала пользователи могут не только оперативно получать необходимую информацию, но и эффективно взаимодействовать с другими участниками бизнес-процесса. Для аутентификации пользователей при доступе к ресурсам системы используются электронные ключи eToken.

Возможности

- Предоставление доступа к необходимой корпоративной информации для всех авторизованных пользователей через единый web-интерфейс.
- Создание единого виртуального каталога хранения корпоративной информации – документного хранилища.
- Интеграция унаследованных данных и приложений.
- Обеспечение прозрачных схем управления потоками информации и публикации.
- Формирование набора сервисов портала в соответствии с индивидуальными информационными потребностями сотрудников.
- Назначение прав доступа производится Администратором портала.
- Возможность оперативно отслеживать состояние сервисов портала с помощью системы мониторинга.
- Возможность использования одного ключа eToken для работы с другими приложениями.



Город-Инфо
(095) 777-7800
info@gorod.ru
www.gorod.ru

eToken Internet Logon

Защищенный удаленный доступ к сети Интернет, защищенный dial-up

- Защита от кражи пароля доступа в Интернет
- Хранение логинов, паролей и параметров соединения в защищенной памяти ключа
- Удобство управления и контроль доступа в Интернет
- Двухфакторная аутентификация пользователя при соединении с провайдером

Назначение

eToken Internet Logon обеспечивает защиту от хищения пароля доступа к сети Интернет по коммутируемым каналам. Основные параметры подключения к различным провайдерам (логин, пароль, телефоны провайдера) хранятся в защищенной области электронного ключа eToken.

Возможности

- Хранение параметров соединения в защищенной области eToken предотвращает возможность их похищения и использования злоумышленником.
- Упорядочивание процедуры доступа в Интернет в рамках организации. Сотрудники могут записать пароль на листке бумаги и приклеить к монитору, могут сообщить его знакомым или воспользоваться для доступа из дома. С eToken Internet Logon вы застрахованы от этого – пароль становится материальным, и его использование можно эффективно контролировать.
- Решение удобно и практично – eToken подключается к USB-порту, который есть почти на каждом компьютере.
- Высокий уровень защиты обеспечивается двухфакторной аутентификацией – подключением eToken и набором PIN-кода.

Системные требования

Windows 9x, ME, NT, 2000

Продукт выпущен в рамках совместного проекта компаниями «Инфотех» и Aladdin Software Security R.D.

Инфотех
(0922) 32-37-68
it@infotech.elcom.ru



Аладдин Р. Д.
(095) 231-3113 (30 линий)
aladdin@aladdin.ru
www.aladdin.ru



Застава

Семейство продуктов для создания защищенных виртуальных частных сетей (VPN) для крупных предприятий

- Защита передаваемой по сетям информации
- Контроль доступа в защищаемый периметр сети
- Идентификация и аутентификация пользователей и сетевых объектов
- Управление политикой сетевой безопасности организации

Назначение

ЭЛВИС+ представляет целостный масштабируемый ряд продуктов семейства «Застава» для создания защищенных виртуальных частных сетей (VPN) между географически разнесенными локальными вычислительными сетями пользователей и подключение к ним удаленных клиентов. «Застава» состоит из VPN-продуктов, устанавливаемых в контрольных точках сети (Клиент–Сервер–Шлюз), и продуктов управления корпоративной VPN.

Возможности

- Защита прозрачна для всех сетевых сервисов и прикладных программ, практически не требует внесения изменений в телекоммуникационную инфраструктуру и топологию сети.
- Подключение внешних криптомодулей производится через Open CryptoAPI интерфейс.
- Цифровые сертификаты стандарта X.509 для подключения удаленных VPN-клиентов и конфигурации локальной политики безопасности сохраняются в защищенной памяти электронного ключа eToken. Этим достигается существенное повышение уровня безопасности системы.
- Осуществляется централизованное управление всеми параметрами и функциями системы.
- Сертификаты Гостехкомиссии позволяют использовать продукты семейства «Застава» как в коммерческих, так и в государственных организациях.

Системные требования

Сервер: Windows NT, Solaris/Intel, Solaris/SPARC
Клиент: Windows 95/98, Solaris/Intel, Solaris/SPARC



Элвис+
(095) 531-4633
info@elvis.ru
www.elvis.ru

ViPNet

Семейство продуктов, обеспечивающее безопасную работу в локальных и глобальных сетях

- Организация корпоративной защищенной сети
- Безопасная работа в Интернете
- Защита информационных ресурсов
- Усиленная аутентификация пользователей
- Сертификаты Гостехкомиссии и ФАПСИ

Назначение

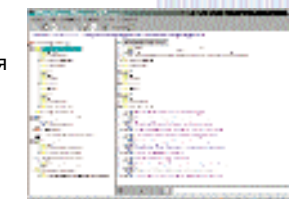
Семейство продуктов ViPNet предназначено для построения защищенных корпоративных сетей, как локальных, так и глобальных. Используемая технология VPN (виртуальных частных сетей) позволяет обеспечить высокий уровень безопасности для пользователей.

Возможности

- Семейство продуктов ViPNet позволяет связывать локальные сети и отдельные рабочие станции в единую защищенную корпоративную сеть. Осуществляется создание виртуальных туннелей между узлами сети за счет шифрования трафика.
- ViPNet обладает свойствами межсетевого экрана и надежно защищает пользователей от попыток внешних атак. Специальные режимы позволяют осуществлять безопасную работу с внешними ресурсами Интернета.
- Наличие сертификатов Гостехкомиссии и ФАПСИ позволяет использовать ViPNet в государственных и иных структурах, где законодательство требует применения сертифицированных средств защиты от несанкционированного доступа.
- С помощью ViPNet обеспечивается электронный документооборот с применением электронно-цифровой подписи.
- Корпоративная сеть защищается от хищения конфиденциальной информации внутри офиса путем организации внутренней структуры корпоративной сети и распределения различных уровней доступа к информации между сотрудниками компании.
- Обеспечивается безопасный доступ к ресурсам сетей общего пользования.
- Аутентификация производится при помощи электронных ключей eToken, что гарантирует высокий уровень безопасности системы и удобство работы мобильных пользователей.

Системные требования

Windows 9x, NT, 2000, Me, Linux



Инфотекс
(095) 737 61 92,
soft@infotecs.ru
www.infotecs.ru



**eToken для Check Point
SecuRemote VPN-1**

Защищенный доступ удаленных клиентов к корпоративной сети

- Аппаратная аутентификация пользователей Check Point SecuRemote/SecureClient версии 4.1 и Next Generation
- Использование цифровых сертификатов X.509
- Разрыв VPN-соединения при отсоединении ключа

Назначение

Check Point SecuRemote – это VPN-клиент, позволяющий удаленным пользователям получить защищенный доступ к необходимым ресурсам корпоративной сети через Интернет. С помощью SecuRemote все данные, передаваемые между удаленным пользователем и защищаемой сетью, шифруются, что гарантирует высокую степень конфиденциальности и целостность данных.

Для работы с данными в сети, защищаемой шлюзом Check Point VPN-1, пользователю достаточно подключить электронный брелок eToken к USB-порту и ввести PIN-код.

Такой метод аутентификации позволяет отказаться от использования паролей, что значительно повышает защищенность VPN и удобство работы.

Возможности

- Использование аппаратной аутентификации вместо паролей при организации VPN-канала.
- Резкое снижение вероятности утери пароля или передачи его третьим лицам.
- Возможность использования единого цифрового сертификата, хранимого в защищенной памяти eToken, для аутентификации VPN-соединения, цифровой подписи и шифрования почтовых сообщений.
- Возможность использования одного eToken различными приложениями.
- Интеграция с большинством серверов цифровых сертификатов.



НПП «БИТ»
(095) 263-42-02
mail@npp-bit.ru
www.npp-bit.ru



Корпорация ЮНИ
(095) 956-6444
uni@uni.ru
www.uni.ru



Аладдин Р. Д.
(095) 231-31-13
aladdin@aladdin.ru
www.aladdin.ru

**Комплексы межсетевого
экранирования «ФПСУ-IP»**

Разграничение доступа в Intranet/Extranet и обеспечение строгой аутентификации пользователей

- Высокий уровень защиты информации
- Строгая двухсторонняя аутентификация пользователей с использованием eToken
- Высокая пропускная способность, быстродействующие VPN туннели
- Тотальный контроль и аудит действий пользователей
- Незаметность применения
- Сертификат Гостехкомиссии при Президенте РФ

Назначение

Комплексы межсетевого экранирования «ФПСУ-IP» предназначены для разграничения доступа в Intranet/Extranet на сетевом и транспортном уровнях в корпоративных сетях и обеспечения строгой аутентификации пользователей.

Возможности

- Построение множественных высокозащищенных туннелей с повышенной пропускной способностью (до 100 Мбит/с) при минимуме стоимости.
- Автоматизированное дистанционное управление и мониторинг состояния системы защиты.
- Обеспечение минимума накладных расходов на организацию туннелей (не более 22 байт на пакет при несжимаемых данных).
- Повышение пропускной способности используемых каналов связи за счет высокоэффективного «проходного» сжатия данных.
- Возможность VPN-поддержки каналов управления пограничными маршрутизаторами организации.
- Адаптивное управление потоками данных при формировании и использовании туннелей.
- Разделение информационных потоков в соответствии с заданными приоритетами.
- Противостояние активным информационным воздействиям разведывательно-диверсионного характера с обеспечением сокрытия топологии защищаемой сети.
- Учет и контроль информационных и управленческих взаимодействий с «неуничтожимыми» следами аудита.

Системные требования

Windows 98, NT, 2000

АМИКОН
(095) 111-93-53
amicon@avallon.ru
www.orc.ru/~amicon



eToken для цифровых сертификатов VeriSign

Защита web-сайтов, приложений и электронной почты

- Безопасные коммуникации через Интернет
- Защита web-сайтов, приложений, электронной почты
- Совместимость с большинством операционных систем
- Хранение сертификата в защищенной памяти eToken

Назначение

Цифровые сертификаты компании VeriSign – это «электронные удостоверения», предназначенные для защиты web-сайтов, приложений, электронной почты от искажения и подделки.

При использовании сертификатов VeriSign и ключей, безопасно хранящихся в eToken, организация может быть уверена в защите своей электронной почты. Сертификаты могут использовать двухфакторную аутентификацию для подписи и расшифровки почтовых сообщений с помощью Microsoft Outlook, Outlook Express и Netscape Messenger. Сертификаты хранятся в памяти eToken и также могут быть использованы для защиты доступа в web через браузеры Internet Explorer и Netscape.

Возможности

- Использование сертификатов гарантирует, что за время передачи данных через Интернет они не были изменены или испорчены.
- Конфиденциальность информации обеспечивается за счет шифрования данных, передаваемых между клиентом и сервером.
- Поддержка сертификатов VeriSign встроена в большинство операционных систем, браузеров и почтовых программ, включая MS Windows и Internet Explorer.

В России процедурой оформления и выдачи сертификатов занимается Департамент интернет-решений РБК через подразделение Thawte компании VeriSign.



РосБизнесКонсалтинг
(095) 363-11-14
solutions@rbk.ru
www.rbk.ru

eToken для системы HP Praesidium PKI (Baltimore UniCERT)

Обеспечение безопасности при работе через Интернет

- Работа с цифровыми сертификатами и личными ключами
- Усиленная аутентификация и PIN-авторизация пользователей
- Хранение сертификатов в защищенной памяти eToken

Компания Hewlett-Packard является стратегическим партнером компании Baltimore Technologies, лидирующей в области технологии PKI.

Назначение

Решения HP Praesidium PKI предоставляют все элементы, необходимые компании для успешного внедрения инфраструктуры PKI.

PKI-система Baltimore UniCERT предназначена для обеспечения безопасности конфиденциальной связи через Интернет, защиты порталов Extranet и Intranet на основе строгой аутентификации пользователей.

UniCERT предлагает всестороннее решение по защите, устанавливая и управляя доверительными отношениями во всех формах электронной коммерции. Используя цифровые сертификаты, UniCERT обеспечивает идентификацию и средства неотракаемости для услуг в следующих типах деятельности: защищенный банковский бизнес через интернет, защищенная почта, покупки через интернет, интерактивная торговля, виртуальные частные сети.

eToken может интегрироваться с:

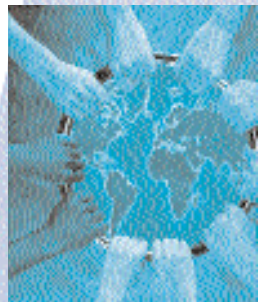
- UniCERT Gateway: Передача и использование сертификатов через e-mail/web
- Baltimore MailSecure: Хранит и использует пользовательские сертификаты для подписывания электронной почты и ее расшифровки (PKCS #11)
- UniCERT Token Manager: Задействует хранение сертификатов на смарт-картах и токенах (PKCS #11)

Компоненты UniCERT взаимодействуют через безопасные соединения TCP/IP (PKIX) используя базы данных Oracle.

Возможности

- Baltimore UniCERT позволяет защищать порталы Extranet и Intranet, используя строгую проверку подлинности пользователей на основе сертификатов.
- Аутентификационные данные пользователя хранятся в eToken, а не на жестком диске компьютера, что значительно снижает риск несанкционированного доступа к ним.
- Высокая защищенность конфиденциальной информации позволяет использовать продукт в электронной коммерции и банковских приложениях.

Hewlett-Packard
(095) 797-35-00
www.software.hp.ru/security
www.hp.com/security



еToken для RSA Keon

Безопасное хранение и работа с цифровыми сертификатами PKI-системы RSA-Keon

- Хранение цифровых сертификатов и личных ключей в еToken
- Снижение риска несанкционированного доступа к сетевым сервисам
- Усиленная аутентификация пользователей

Назначение

RSA Keon – решение, базирующееся на использовании технологии инфраструктуры открытых ключей (PKI). RSA Keon совершенствует защиту для приложений с помощью обеспечения авторизованного доступа к приложению и защищенного шифрованного канала с использованием технологии цифровых сертификатов и строгой двухфакторной аутентификации.

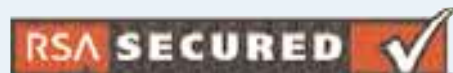
еToken для RSA Keon обеспечивает пользователям PKI-систем программную или аппаратную генерацию личных RSA-ключей (1024 бит) и хранение цифровых сертификатов в защищенной памяти электронного брелка. Этим достигается высокий уровень безопасности и удобства в использовании.

Возможности

- **Keon Security Server** обеспечивает централизованное управление защитой, управление single sign-on доступом к поддерживаемым приложениям, гарантируя прочность системы, ее гибкость и масштабируемость.
- **Keon Desktop** обеспечивает шифрование файлов, управляет single sign-on и правами пользователя на рабочей станции и предоставляет услуги по защите электронной почты, web-браузеров и доступа к приложениям.
- **Keon Agents** устанавливаются на защищаемые серверы приложений и создают аутентифицированное, безопасное подключение рабочей станции к серверу приложений.
- **Keon Agents SDK** дает разработчикам возможность создавать собственное ПО для своих внутренних приложений.
- **Keon Certificate Server** обеспечивает мощную и гибкую систему для создания и управления цифровыми сертификатами.
- **Keon Advanced PKI** – полный набор решений RSA; включает в себя RSA Keon Security Server, RSA Keon Desktop и RSA Keon Certificate Server.
- Сертификаты и личные ключи пользователя хранятся в защищенной памяти еToken, а не на жестком диске компьютера, где они подвергаются риску хищения.



Demos
(095)956-60-80
deg@democ.ru
www.democ.ru



еToken для SAP R/3

Аутентификация пользователя при доступе к системе управления предприятием SAP R/3

- Удобная и безопасная работа в среде SAP R/3
- Хранение сертификатов и паролей
- Подпись и шифрование личных файлов
- Блокирование компьютера или отключение от сети при отсоединении электронного ключа

Назначение

еToken для SAP R/3 позволит отказаться от использования паролей при входе в систему управления предприятием SAP R/3. Пользователям теперь нет необходимости запоминать пароли, периодически их менять и вводить при входе в систему – необходимо лишь подключить электронный брелок еToken к USB-порту и ввести PIN-код. При этом значительно повышаются безопасность и удобство работы.

Возможности

- Вход в сеть и в среду SAP R/3 производится с помощью электронного брелка еToken, аппаратная аутентификация вместо пароля значительно увеличивает безопасность системы.
- Защита личных файлов от несанкционированного доступа, шифрование и цифровая подпись – все это реализовано в еToken для SAP R/3.
- Блокирование компьютера при отсоединении брелка еToken.
- Хранение цифровых сертификатов в защищенной памяти брелка еToken, а не на диске, обеспечивает высокий уровень безопасности.
- Возможность использования одного еToken различными приложениями создает дополнительное удобство для пользователя.

Эффективность защиты напрямую зависит от качества паролей и от количества их введения. При использовании еToken вместо парольной защиты безопасность значительно повышается.



Мекомп
(095) 305-30-90
mecomp@mecomp.ru
www.mecomp.ru

O'KEY 7.7

Усиленная аутентификация пользователей в системе «1С: Предприятие»

- Авторизация документов
- Аутентификация пользователей
- Скрытое ограничение прав доступа
- Сертификат качества компании 1С

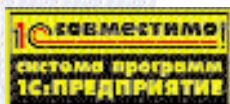
Назначение

«O'KEY 7.7» – это инструмент, который поможет построить целостную систему безопасности деловой информации в системе «1С:Предприятие», избавиться от паролей и не бояться за сохранность корпоративной информации.

Система аппаратной авторизации доступа «O'KEY 7.7» с использованием USB-ключей eToken позволяет обходиться без паролей и авторизовать документы без перезагрузки системы «1С:Предприятие». Работа становится простой, удобной и быстрой. Скрытое разграничение доступа значительно повышает защищенность данных и предотвращает попытки взлома информационных баз.

Возможности

- Двухфакторная аутентификация с помощью ключа и PIN-кода значительно усиливает безопасность системы управления предприятием.
- Осуществляется разграничение прав доступа для пользователей.
- Система обеспечивает авторизацию документов при одновременной работе нескольких сотрудников за одним компьютером.
- Предоставляется возможность проверки присутствия сотрудника на своем рабочем месте.
- Обеспечивается автоматическое отключение/перезагрузка компьютера, закрытие всех форм и окна «1С:Предприятие» при уходе сотрудника со своего рабочего места.
- Встраивается в любую конфигурацию системы «1С: Предприятие 7.5/7.7»



1-й Архитектор бизнеса
(095) 720-60-22
info@1ab.ru
www.1ab.ru

eToken для Documentum 4i

Усиленная аутентификация пользователей в промышленной платформе для создания распределенных систем управления информационным содержанием корпоративных интернет-сайтов и интранет-порталов

- Снижение риска несанкционированного доступа к системе
- Аппаратная аутентификация пользователей вместо ввода паролей
- Удобство работы в системе Documentum 4i

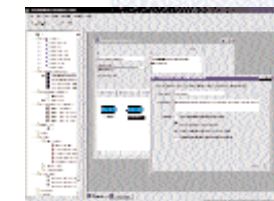
Назначение

Платформа Documentum 4i ориентирована на крупные предприятия, имеющие большое количество пользователей, документов и задач, связанных с хранением информации, ее обработкой и публикацией на корпоративных интернет-сайтах и информационных порталах.

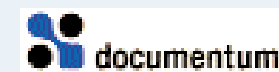
Электронный ключ eToken для Documentum 4i значительно облегчает и делает безопасным процесс доступа к информационным ресурсам. Пользователю не нужно запоминать сложные пароли – достаточно подключить eToken и ввести PIN-код.

Возможности

- Двухфакторная аутентификация пользователя системы Documentum 4i гарантирует высокий уровень безопасности при работе с системой.
- Удобство работы с eToken заключается в том, что теперь пользователям системы Documentum нет необходимости запоминать сложные пароли для доступа к ресурсам. Для работы требуется подключение eToken к USB-порту компьютера и введение PIN-кода.
- Хранение пароля в eToken существенно повышает уровень контроля доступа к информационным ресурсам.
- Использование электронных ключей значительно снижает вероятность кражи паролей и возможность несанкционированного доступа к ресурсам системы Documentum.
- eToken, используемый для работы с системой Documentum 4i, также может использоваться и другими приложениями.



Документум Сервисиз
(095) 737-8089, 737-8009.
elena.strelkova@documentum.ru
www.documentum.ru



eToken для DOCS Open

Усиленная аутентификация пользователей в системе управления документами

- Двухфакторная аутентификация пользователей
- Удобство и безопасность работы с системой управления документами
- Разграничение прав доступа для групп и отдельных пользователей

Назначение

Система предназначена для создания электронных хранилищ, архивов, для работы с инженерно-конструкторской и нормативно-справочной документацией масштаба среднего предприятия.

eToken для DOCS Open обеспечивает удобство и высокий уровень безопасности при работе с системой управления документами DOCS Open. Информация о пользователе, необходимая для аутентификации, хранится в защищенной памяти электронного брелка eToken.

Возможности

- **Регистрация документов и поручений.** Организация работы управления делами, канцелярий, экспедиций.
- **Работа с документами и их версиями.** Упрощение и упорядочивание работы с документами, организация внутреннего документооборота, а также построение корпоративного хранилища неструктурированной информации.
- **Атрибутивный и полнотекстовый поиск** в локальных и удаленных библиотеках. Возможность быстро найти необходимый документ и просмотреть его встроенными средствами с подсветкой запрашиваемых слов.
- **Выписка и возврат документов** для работы вне корпоративной сети. Локальная работа с документами вне системы.
- **Ведение истории работы с документом.** Реализация полного аудита доступа к документам и работы пользователей.
- **Разграничение прав доступа** для групп и отдельных пользователей. Сотрудникам доступна только та информация, которая необходима им для работы.
- **Отказ от использования паролей** для доступа в систему управления документами и замена их на более надежную двухфакторную аутентификацию с помощью электронного ключа eToken и PIN-кода.
- **Защита документов** с использованием электронной цифровой подписи (ЭЦП).

Разработчик DOCS Open и CyberDOCS – компания Hummingbird (Канада).
Единственный мастер-реселлер в России – компания «Вест-МетаТехнология».

Вест-МетаТехнология
(095) 115-6001
hummingbird@vest.msk.ru
www.vest.msk.ru



eToken для CyberDOCS

Усиленная аутентификация пользователей в web-ориентированной системе управления документами

- Высокий уровень безопасности системы
- Двухфакторная аутентификация пользователей
- Удобство работы с web-ориентированной системой управления документами

Назначение

CyberDOCS фирмы Hummingbird предоставляет пользователям все функциональные возможности системы управления документами через интерфейс стандартного web-браузера и работает как в Интернете, так и во внутрикорпоративной сети интранет. Из любого браузера сотрудники, клиенты и поставщики могут легко находить нужные им документы, располагающиеся в электронных хранилищах, и изменять эти документы в соответствии с имеющимися у них правами в течение всего жизненного цикла документа.

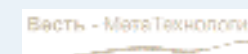
eToken для CyberDOCS обеспечивает высокий уровень безопасности при работе с web-ориентированной системой управления документами CyberDOCS. Чтобы получить доступ к системе, пользователь должен подключить к USB-порту электронный ключ eToken и ввести корректный PIN-код.

Возможности

- Удобная организация работы с документами – организует работу с имеющимися документами, объединяет все документы предприятия в стройную систему.
- Свободная маршрутизация документов и заданий с контролем исполнительской дисциплины.
- Исключение возможности потери документа – один раз попав в систему, документ не может из нее исчезнуть.
- Высокоэффективный поисковый механизм позволяет производить как полнотекстовый поиск, так и поиск по ключевым словам.
- Отказ от использования паролей для доступа в систему управления документами и замена их на более надежную аппаратную аутентификацию с помощью USB-ключей eToken.
- Высокий уровень безопасности при работе с системой через Интернет за счет использования двухфакторной аутентификации.
- Проверка прав доступа к документам и защита документов с использованием электронной цифровой подписи (ЭЦП).

Разработчик DOCS Open и CyberDOCS – компания Hummingbird (Канада).
Единственный мастер-реселлер в России – компания «Вест-МетаТехнология».

Вест-МетаТехнология
(095) 115-6001,
hummingbird@vest.msk.ru
www.vest.msk.ru



Защищенная система управления распределенной сетью торговых предприятий с центральной базой данных

- Надежность и отказоустойчивость
- Высокий уровень безопасности и удобство работы
- Аутентификация пользователей и разграничение доступа с использованием eToken
- Одновременная работа с большим количеством удаленных клиентов

Назначение

Предлагаемое техническое решение представляет собой технологию создания систем учета деятельности торговых предприятий с центральной базой данных. Предназначено для дистрибуторских, MLM (multilevel-marketing) компаний, организаций, работающих с персонализированными базами данных. Доступ к системе осуществляется в защищенном режиме с использованием электронных ключей eToken с удаленных рабочих мест, подключенных к сети Интернет.

Возможности

- Система имеет трехуровневую архитектуру (сервер базы данных, сервер приложений, клиентское ПО) и гарантирует высокую степень надежности и отказоустойчивости в работе.
- Клиентские модули работают в реальном режиме времени и требуют только наличия MS Internet Explorer, поставляемого с любой современной версией MS Windows.
- Использование электронных ключей eToken обеспечивает разграничение доступа для разных категорий пользователей.
- Большая эффективность отдачи от вложенных средств реализуется за счет работы через Интернет вместо использования сети выделенных каналов.

Решение применено в реально функционирующей автоматизированной информационной системе международного фармацевтического холдинга, где более полумиллиона клиентов, дилеров и партнеров компании имеют возможность подключаться к серверам холдинга, что значительно сокращает временные затраты и повышает эффективность бизнеса.

Системные требования

WEB-сервер: любой из существующих WEB-серверов (APACHE, IIS и др.)
Сервер базы данных: любой SQL-сервер (MS SQL, InterBase, Oracle и др.)



ВИП-Телеком
(095) 927-80-46
telecom@vip-rus.com
www.vip-telecom.net

Matrix

Система управления доступом к информации и функциям защищаемых автоматизированных систем

для администраторов безопасности и разработчиков корпоративных систем

- Защита информации от несанкционированного доступа
- Централизованное хранение правил разграничения доступа
- Программно-аппаратная авторизация пользователей
- Гибкая настройка правил разграничения доступа
- Контроль доступа к объектам разных типов

Назначение

Администратор информационной безопасности с помощью графического интерфейса Matrix сможет легко управлять доступом к информации и функциям защищаемых автоматизированных систем. Разработчики автоматизированных систем, которым необходимо обеспечить разграничение доступа к информации в своих системах, смогут существенно снизить трудоемкость процесса выполнения требований по защите информации и повысить защищенность своих систем за счет интеграции с Matrix. Разработчику нужно будет лишь вставить в свой код обращение к функциям API Matrix и описать с помощью графического интерфейса все возможные операции в своей системе, доступ к которым должен быть разграничен. Для соблюдения установленных правил безопасности пользователям автоматизированных систем, защищаемых Matrix, не надо запоминать сложных паролей и заботиться об их периодической смене. Пользователю достаточно будет вставить eToken в USB-разъем компьютера, и Matrix сможет идентифицировать пользователя и определить все доступные для него элементы интерфейса. При этом повышается защищенность системы и удобство работы.

Возможности

- Гибкая настройка администратором безопасности правил разграничения доступа в таких терминах, как: пользователь; служебная обязанность; технологическая операция в системе.
- Единое средство для формирования прав доступа к объектам различных типов: таблицам и представлениям в базах данных, файлам и каталогам, а также ресурсам Интернета.
- Динамическая настройка элементов экранного интерфейса в защищаемой программе (доступность кнопок, переключателей и пунктов меню), которая выполняется в зависимости от прав текущего пользователя на выполнение технологических операций в системе.
- Хранение ключей шифрования для базы правил разграничения доступа в защищенной памяти eToken, а не на диске.
- Соответствие требованиям руководящих документов Гостехкомиссии при Президенте РФ по защите информации от несанкционированного доступа.

Программное обеспечение Matrix разрабатывается ЛАНИТ в соответствии со стандартом обеспечения качества ISO 9001.

ЛАНИТ
967-66-50
systems@lanit.ru
systems.lanit.ru



Электронный замок eToken PC-Lock

Защита персонального компьютера от несанкционированной начальной загрузки

Уникальная технология!

- Усиленная аутентификация пользователя при загрузке компьютера
- Замена парольной защиты BIOS на более надежную – аппаратную
- Возможность блокирования загрузки со съемных дисков
- Ведение журнала регистрации

Электронный замок препятствует загрузке компьютера посторонними лицами. Чтобы получить доступ к компьютеру, после включения пользователь должен подключить к USB-порту электронный ключ eToken и набрать (опционально) PIN-код. Компьютер загрузится, если только подключен «правильный» брелок и набран корректный код.

Назначение

- Предотвращение несанкционированного доступа к информации, хранящейся в компьютере.
- Обеспечение доступа к информации, хранящейся в компьютере, только законным владельцам, имеющим электронный ключ eToken и знающим его PIN-код.
- Недопущение установки на компьютер в отсутствие хозяина программ-шпионов с целью перехвата хранящейся в компьютере конфиденциальной информации.

Возможности

- Простота подключения: достаточно подключить ключ к USB-порту и набрать PIN-код.
- Один ключ может использоваться различными приложениями.
- Многопользовательский доступ. Замок позволяет иметь для одного компьютера несколько ключей, в т.ч. можно изготовить универсальный ключ Администратора.
- Можно обеспечить нескольким пользователям возможность работать с одним компьютером: каждый пользователь должен иметь свой уникальный ключ.
- Один пользователь с одним ключом может работать на разных компьютерах.

Возможная реализация:

- запись кода замка в BIOS (перепрограммирование BIOS);
- установка ПЗУ с кодом замка в сетевую карту, имеющую свободную панельку для BootROM.



Аладдин Р. Д.
(095) 231-3113 (30 линий)
aladdin@aladdin.ru
www.aladdin.ru

Crypton Lock

Управление доступом к рабочим станциям в локальных сетях

- Аутентификация пользователя с помощью eToken
- Контроль доступа к рабочим станциям
- Высокий уровень безопасности при работе пользователей
- Централизованное формирование паролей

Назначение

Разграничение доступа пользователей к рабочим станциям в локальных сетях в соответствии с политикой безопасности организации. Обеспечение высокого уровня защищенности информационных ресурсов за счет использования электронных ключей eToken.

Возможности

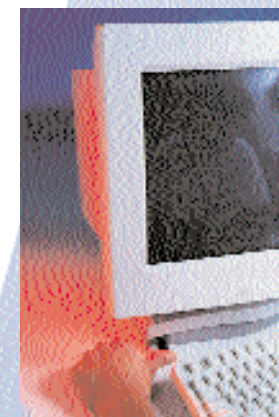
- Хранение пароля в защищенной памяти электронного ключа eToken.
- Вход в систему только зарегистрированных пользователей после предъявления eToken. Администратору безопасности достаточно один раз ввести пароли в память электронных ключей и раздать их пользователям; сообщать пароли пользователям не нужно.
- Пароль становится материальным, его можно хранить и учитывать, как любой материальный объект.
- Централизованное формирование паролей значительно повышает уровень общей безопасности сети.
- Блокировка системы на время отсутствия оператора на рабочем месте существенно повышает уровень защиты от несанкционированного доступа.

Системные требования

Windows NT 4.0, 2000.



При покупке электронного ключа eToken в фирме АНКАД предоставляется возможность также хранить в его памяти ключи шифрования и электронной цифровой подписи для продуктов серии КРИПТОН/Crypton: КРИПТОН-Шифрование, КРИПТОН-Подпись, Crypton ArcMail, Crypton Word, Crypton Excel.



АНКАД
(095) 531-0000
marketing@ancud.ru
www.ancud.ru



Secret Disk Система защиты конфиденциальной информации

- «Прозрачное» шифрование обрабатываемой информации
- Аппаратная аутентификация пользователей «секретных» дисков
- Возможность мгновенного блокирования системы
- Сертификат Гостехкомиссии

Защищая информацию, мы защищаем свой бизнес

Назначение

Secret Disk превратит компьютер в чемоданчик с двойным дном, даст ему вторую, скрытую от посторонних жизнь. Ключом от нее является eToken, который позволяет компьютеру отличить «своего» от «чужого», открыть «второе дно» компьютера и получить доступ к его скрытым ресурсам. Secret Disk создает в компьютере новые, «секретные» диски. При сохранении на них информация автоматически шифруется. Чтобы использовать такой диск, необходимо подключить электронный ключ и ввести пароль. Подключить секретный диск без ключа и пароля нельзя – для посторонних он останется просто незаметным файлом.

Возможности

- Безопасная работа, хранение и передача конфиденциальной информации.
- Аппаратная идентификация пользователей с помощью электронных ключей eToken.
- Возможность использования мощных криптоалгоритмов, в том числе сертифицированных ФАПСИ.
- Мгновенное «уничтожение» информации при подаче сигнала «тревога» и при «входе под принуждением».
- Блокирование компьютера в перерывах между работой.
- Создание защищенных архивов.
- Простота и удобство в работе.

Secret Disk позволяет подключать внешние модули криптографической защиты, например, входящие в Windows, или эмулятор известной платы «Криптон», реализующей мощный российский алгоритм шифрования ГОСТ 28147-89 с длиной ключа 256 бит.

Системные требования

Windows 9x, Me, NT, 2000

Аладдин Р. Д.
(095) 231-3113 (30 линий)
aladdin@aladdin.ru
www.aladdin.ru



eToken – ключ эпохи Интернет

Полнофункциональный аналог смарткарты в виде USB-брелка

- Аутентификация пользователя при доступе к защищенным ресурсам
- Безопасное хранение ключей шифрования, цифровых сертификатов, секретных данных
- Обеспечение безопасности финансовых транзакций

Что такое eToken?

eToken – это полнофункциональный аналог смарткарты, выполненный в виде брелка. Он напрямую подключается к компьютеру через порт USB (Universal Serial Bus) и не требует наличия дорогостоящих карт-ридеров или других дополнительных устройств. eToken имеет до 64Кбайт защищенной памяти и может использоваться как портативный контейнер для хранения ключей шифрования, кодов доступа, сертификатов и пр. eToken имеет открытую архитектуру и интегрируется со всеми основными системами, использующими технологию PKI (Public Key Infrastructure).

eToken R2 имеет аппаратно реализованный алгоритм шифрования DESX/120.

eToken Pro имеет дополнительный чип смарткарты, аппаратно реализующий криптоалгоритмы RSA/1024, TripleDES, SHA-1 и генератор личных ключей, никогда не покидающих чип.

eToken RIC имеет аппаратно реализованные криптоалгоритмы DES, TripleDES и ГОСТ 28147-89 (сертифицирован ФАПСИ); поддерживает диверсификацию и формирование сессионного ключа. Встроенная виртуальная машина позволяет расширять и модифицировать систему команд eToken RIC для поддержки различных приложений, включая платежные и другие системы.

Назначение

- Аутентификация пользователя при доступе к защищенным ресурсам.
- Безопасное хранение ключей шифрования, цифровых сертификатов, любой другой секретной информации.
- Обеспечение безопасности финансовых транзакций.

Возможности

- Усиленная аутентификация пользователей при доступе к базам данных, серверам, защищенным страницам web-сайтов.
- Защита сетей и компьютеров, электронной почты, VPN.
- Клиент-банк, home-banking, электронная торговля.
- Платежные интернет-системы.

eToken RIC разработан компанией Aladdin Software Security R.D. и ИТЦ «АТЛАС»

Аладдин Р. Д.
(095) 231-31-13
security@aladdin.ru
www.aladdin.ru



КриптоПро CSP

Средство криптографической защиты информации в формате MS CSP

- Обеспечение конфиденциальности и контроля целостности информации
- Авторизация электронных документов при помощи цифровой подписи
- Криптографический интерфейс CryptoAPI
- Хранение цифровых сертификатов в памяти eToken, PIN-авторизация
- Сертификат ФАПСИ

Назначение

КриптоПро CSP предназначено для:

- авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями посредством использования процедур формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии с отечественными стандартами ГОСТ Р 34.10–94, ГОСТ Р 34.11–94;
- обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты в соответствии с ГОСТ 28147–89;
- контроля целостности, системного и прикладного программного обеспечения для его защиты от несанкционированного изменения или от нарушения правильности функционирования;
- управления ключевыми элементами системы в соответствии с регламентом средств защиты.

Возможности

КриптоПро CSP позволяет использовать российские криптографические алгоритмы и сертификаты открытых ключей X.509 со следующим программным обеспечением:

- Центр Сертификации – Microsoft Certification Authority, входящий в состав OS Windows 2000 Server, Advanced Server.
- Электронная почта – Microsoft Outlook 98, 2000, XP, Microsoft Outlook Express.
- Средства контроля целостности ПО, распространяемого по сети – Microsoft Authenticode.
- Защита TCP/IP соединений в сети Интернет – протокол TLS/SSL при взаимодействии Internet Explorer – Web сервер IIS 5.0 (4.0).
- Цифровые сертификаты хранятся в защищенной памяти USB-ключей eToken, что повышает удобство и мобильность работы.

Системные требования

Windows 9x, ME, NT, 2000.



Крипто-Про
(095) 289 4367
info@cryptopro.ru
www.cryptopro.ru

КриптоТраст

Программы и технологии для Центров Сертификации и Регистрации

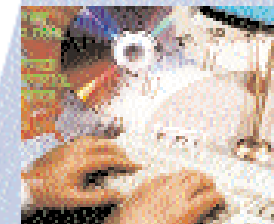
- Надежная и удобная техника управления цифровыми сертификатами в системах электронной торговли, документооборота и электронных расчетов
- Поддержка цифровых сертификатов X.509, их хранение в защищенной памяти eToken
- Простые и удобные технологии управления
- Сертификаты Госстандарта РФ на модули для работы с электронными документами

Назначение

«Центр Сертификации» и «Центр Регистрации» – программы контроля подлинности персональных идентификаторов пользователей (в системах клиент–банк и электронной коммерции, корпоративных сетях). Основой Цифровой Сертификации является электронный паспорт (сертификат). Он содержит данные о пользователе, образец его цифровой подписи и открытую часть его персонального идентификатора. Центры занимаются выдачей, регистрацией и контролем цифровых сертификатов и являются гарантами их подлинности. Для работы с пользователями в нескольких регионах (странах) используются «Центры Регистрации», через которые подтверждаются данные о пользователях и заявках на сертификаты.

Возможности

- Надежные и эффективные алгоритмы цифровой подписи, защиты данных, генерации и управления индивидуальными числами–ключами пользователей с детальным описанием и точным математическим обоснованием их надежности.
- Максимально удобные и понятные для пользователя прикладные программы.
- Библиотека разработчика для включения функций цифровой подписи и защиты данных и сообщений непосредственно в приложения.
- Полное и детальное описание взаимодействия сторон при работе с цифровыми сертификатами и электронными документами и сообщениями, подписанными цифровой подписью и защищенными от просмотра при передаче.
- Точные ссылки на все действующие законы и другие нормативные документы Российской Федерации, регулирующие применение таких технологий.



ЛАН Крипто
(095) 288–50–56, 288–53–88
lanc@aha.ru
www.lancrypto.com

Система Интернет–Платежей Instant Obtain

- Оплата в режиме on–line товаров (услуг), приобретаемых через интернет–магазины
- Удаленная инкассация накопленных средств Продавца в банк
- Подтверждение произведенной оплаты для автоматизированной системы Продавца
- Обеспечение защиты данных в сети Интернет, строгая аутентификация участников расчетов

Назначение

Система предназначена для реализации электронных платежей через Интернет с использованием микропроцессорных карт стандарта DUET (СБЕРКАРТ). Технология микропроцессорных банковских карт, а также аппаратные средства защиты программного обеспечения и передаваемых данных обеспечивают проведение финансовых транзакций с максимально возможным уровнем безопасности. eToken способен заменить дорогостоящие карт–ридер, смарткарту и аппаратные средства защиты платежных приложений. Клиенты системы со своего рабочего места могут оплачивать доступ к платным ресурсам Сети, совершать покупки в интернет–магазинах, осуществлять безналичные платежи произвольного назначения. Система позволяет клиенту удаленно выполнять стандартные сервисные операции – просмотр баланса и истории карты, загрузка средств, перевод средств с защищенного на открытый остаток карты, смена паролей, авторизация и др.

Преимущества

- Максимальная защищенность финансовых средств.
- Быстрота и простота процедуры оплаты.
- Общедоступное средство платежа.
- Аппаратные средства защиты данных и программ.
- Возможность использования eToken вместо смарткарты для проведения финансовых транзакций.

Системные требования

Сервер: Windows NT

Клиент: Windows 9x, NT, Internet Explorer v.4.0 SP2 и выше

СмартКарт–Сервис
234–3168
managers@scserv.ru
www.scserv.ru

Кварт Технологии

Интеграция систем информационной безопасности

- Комплексный анализ информационных систем
- Разработка крупных информационных комплексов
- Интеграция систем защиты информации
- Развертывание и настройка корпоративных PKI систем

Назначение

«Кварт Технологии» – это команда высококвалифицированных специалистов, оказывающих услуги по разработке, интеграции и сопровождению больших информационных систем с интегрированными подсистемами информационной безопасности.

Возможности

- Системный анализ информационных систем.
- Разработка крупных компьютеризированных комплексов, в том числе по информационной безопасности.
- Развертывание корпоративных серверов сертификатов MS CA.
- Разработка и настройка политик безопасности в сетях Windows 2000.
- Внедрение и настройка средств аппаратной аутентификации в сетях Windows 2000.
- Установка программно–аппаратных средств защиты информации.
- Разработка защищенных web–сайтов.
- Разработка распределенных сетей с защищенным обменом информацией.
- Разработка и внедрение систем разграничения доступа.



Кварт Технологии
(095) 234–4018
info@quarta.com
www.quarta.ru

Служба F1

Сервисная поддержка систем информационной безопасности

Нам доверяют!

- Аудит и обслуживание информационных систем
- Установка и настройка программно-аппаратных средств безопасности
- Защита и восстановление данных
- Обучение персонала

Назначение

Служба F1 – это команда сертифицированных специалистов, оказывающих широкий спектр услуг по установке, наладке и сопровождению программно-аппаратных средств обеспечения информационной безопасности.

Возможности

- Предоставление технических консультаций по телефону.
- Диагностика компьютерных систем.
- Аудит и обслуживание информационных систем.
- Устранение конфликтов в работе информационных систем.
- Идентификация и уничтожение компьютерных вирусов.
- Защита информации от несанкционированного доступа.
- Установка программно-аппаратных средств защиты информации.
- Восстановление данных.
- Создание защищенных Web-сайтов.

Основное правило работы Службы F1 – качественное решение проблем на территории Заказчика в удобное время и по разумной цене.

Учебный Центр "ИНФОРМЗАЩИТА"

Подготовка специалистов в области информационной безопасности

Учебный Центр «ИНФОРМЗАЩИТА» осуществляет подготовку по программе дополнительного профессионального образования (повышения квалификации) специалистов, работающих в области технической защиты информации и обеспечения информационной безопасности автоматизированных систем. В рамках сотрудничества с компанией «Аладдин» Учебный Центр «Информзащита» проводит курс «Теория и практика PKI». Программа учебного курса ориентирована на специалистов в области защиты информации, ответственных за администрирование средств построения инфраструктуры открытых ключей (Public Key Infrastructure – PKI), а также планирующих их внедрение.

В рамках курса рассматриваются теоретические основы, организационно-правовые вопросы применения средств криптографической защиты информации, стандарты и варианты практических подходов к построению инфраструктуры открытых ключей, подробно анализируются различные решения, на основе которых строятся PKI, обсуждаются достоинства и недостатки различных вариантов реализации PKI. Особое внимание уделяется вопросам реализации инфраструктуры открытых ключей на платформе MS Windows 2000 с учетом российской специфики. В ходе практических занятий отрабатываются задачи, необходимость решения которых возникает при внедрении PKI, слушатели приобретают навыки по установке, настройке и администрированию средств построения PKI на базе MS Windows с использованием сертифицированного криптопровайдера КриптоПРО CSP и электронных ключей eToken.



Авторизованный Учебный Центр «САМАН»*Обучение и подготовка сертифицированных специалистов*

Авторизованный Учебный Центр ЦОИТ «САМАН» проводит сертифицированные учебные курсы по продуктам компании «Аладдин». Учебные курсы ориентированы на подготовку сертифицированных дилеров, продвигающих разработки компании, а также на специалистов, которые стремятся повысить свои навыки при работе с широким спектром продуктов компании «Аладдин».

Основные направления обучения:

- системы защиты корпоративной информации Secret Disk / Secret Disk Server;
- специализированные курсы по технологиям защиты программ и данных, построенные на решениях компании «Аладдин».

В 1993 году в ЦОИТ «САМАН» открыт первый в СНГ центр тестирования специалистов компании Sylvan Prometric. В настоящее время ЦОИТ «САМАН» является крупнейшим в СНГ центром тестирования и сертификации. С 1996 года центр является Сетевым Партнером Novell. В 1999 году ЦОИТ «САМАН» получил статус Авторизованного Учебного Центра компании Aladdin Software Security R.D.



Учебный центр ЦОИТ «САМАН»
(095) 915-3358, 915-3580, 915-7124
postmaster@education.ru
www.education.ru

ALERO Software Alliance B.V.*Издание и продвижение решений по информационной безопасности*

- Издание продуктов по информационной безопасности
- Локализация продуктов для западных рынков
- Проведение комплекса маркетинговых мероприятий
- Продвижение продуктов на западных рынках

Назначение

Основная деятельность компании ALERO Software Alliance B.V. – издание программных продуктов по информационной безопасности, маркетинг и продвижение изданных продуктов на западном рынке. Компания имеет штат квалифицированных сотрудников, имеющих опыт продаж систем информационной безопасности на рынках разных стран.

Возможности

- Анализ рынка систем информационной безопасности.
- Разработка дизайна программных продуктов: коробки, документации, рекламные листовки и буклеты.
- Тиражирование программных продуктов.
- Проведение рекламных кампаний в различных странах.
- Сертификация издающихся программных продуктов на местных рынках.

**Alero Software Alliance B.V.**

Московский офис:
(095) 937-9436
info@alero-software.com
www.alero-software.com

Голландский офис:
+31 20 667 0168
info@alero-software.com
www.alero-software.com



Проект InfoSecurity.ru



Сетевая газета и проблемно–ориентированный сайт по информационной безопасности

- Освещение вопросов информационной безопасности
- Новости рынка систем обеспечения информационной безопасности
- Обзор программно–аппаратных средств защиты

Назначение

Обсуждение вопросов, связанных с информационной безопасностью бизнеса. Освещение проблем, методов и решений в сфере информационной безопасности. Информирование о программно–аппаратных средствах защиты информации.

Содержание

- Виды угроз.
- Способы обеспечения информационной безопасности.
- Методы обеспечения информационной безопасности.
- Анализ защищенности информации.
- Разработка концепции.
- Выбор средств защиты информации.
- Применяемые решения и их анализ.
- Новости, статьи и пресс–релизы.
- Ответы на вопросы.

Партнерская программа

Все подписавшиеся на рассылку сетевой газеты InfoSecurity.ru получают виртуальную дисконтную карту Службы F1.

Проект InfoSecurity.ru
(095) 231–4831 (многоканальный), 366–8883
f1@f1.com.ru
www.InfoSecurity.ru

