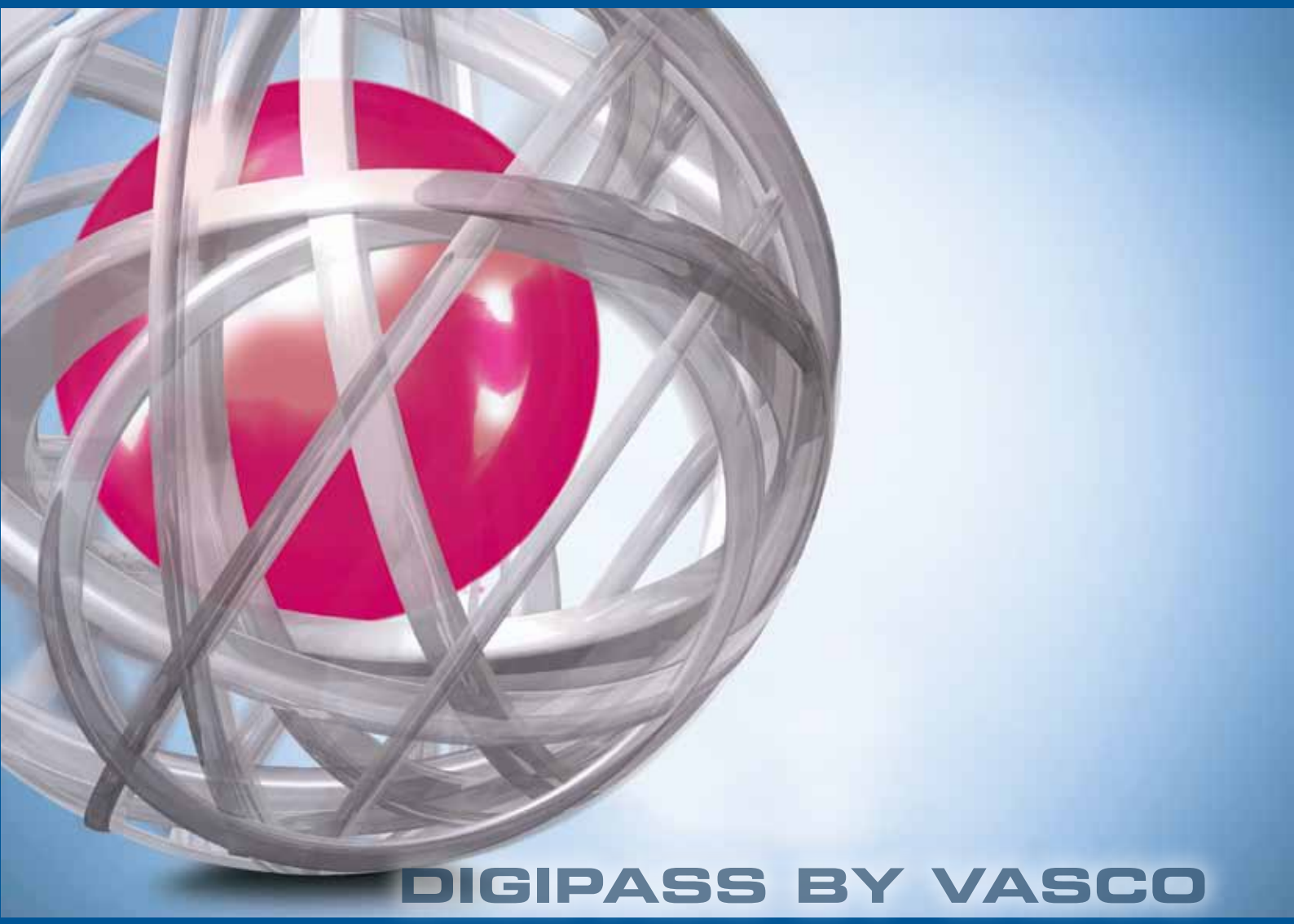
Сервер IDENTIKEY

Сервер аутентификации VASCO следующего поколения



VASCO
THE AUTHENTICATION COMPANY

Ведущий мировой поставщик решений по обеспечению **Интернет-безопасности**

ЗАЩИТИ СВОЙ БИЗНЕС

Сегодня деятельность любой компании всё больше зависит от ежедневных операций в сети Интернет. Вопросы безопасности стали одинаково насущными как для администраторов сетей, так и для банков. Стоит ли вопрос о защите удаленного доступа к корпоративным сетям, бизнес-приложениям, либо речь идет о финансовых транзакциях в режиме онлайн, компании пребывают под постоянной угрозой атак со стороны онлайн-мошенников.

Все больше предприятий рассматривают возможности перехода на сетевые хост-приложения, также известные под названием SaaS или как приложения по требованию. Приложение предоставляется в качестве отдельной услуги и запускается из пользовательского Интернет-браузера. Как правило, работа с такими приложениями не требует каких-либо дополнительных программно-аппаратных средств и обходится пользователю довольно дешево. С переходом на сетевые хост-приложения администраторы сетей, как правило, задумываются о безопасности важных данных, сохраняемых в таких приложениях. Насколько велика степень защиты данных, скажем, бухгалтерии в Интернет-приложениях? Надежно ли защищена важная информация в руках третьих лиц? Защищен ли доступ к конфиденциальным данным от несанкционированного вторжения?

ПЕРЕХОД ОТ СТАТИЧЕСКОГО ПАРОЛЯ К ДИНАМИЧЕСКОМУ (OTP)

К сожалению, статические пароли уже не обеспечивают надежную защиту от кражи данных, фишинга или MITM-атак. Статический пароль можно легко угадать, копировать, распространять, передавать и использовать в мошеннических целях. Простые пароли очень легко запоминаются, но они не гарантируют безопасность. Сложные пароли более безопасны, но их часто записывают, что снижает степень защиты. Преимущества двухфакторной аутентификации как противодействия хакерским атакам и мошенничеству доказаны уже не раз.

Являясь мировым разработчиком решений в области двухфакторной аутентификации, VASCO® Data Security обеспечивает надежные технологии при минимальном воздействии на общую IT-архитектуру. Решения VASCO рассчитаны на усиление действующих мер безопасности. Такие решения были опробованы и значительно улучшены за многолетний период использования в банковском секторе.

УСТРОЙСТВА VASCO DIGIPASS

Семейство продуктов DIGIPASS® разработки VASCO используется ведущими мировыми банками и может считаться эталоном безопасной аутентификации. На замену устаревшим и небезопасным статическим паролям пришли динамические пароли, действительные однократно, и электронная подпись данных, что значительно улучшило защиту онлайн-транзакций. Предлагая продукты запатентованной марки IDENTIKEY®, компания VASCO вводит в обиход двухфакторную аутентификацию, обеспечивая такой же высокий уровень безопасности для предприятий, который используется в финансовом мире для защиты от несанкционированного доступа к приложениям.

Сервер IDENTIKEY

Сервер IDENTIKEY является централизованным сервером следующего поколения с поддержкой технологий аутентификации DIGIPASS. Он используется для подтверждения запроса на аутентификацию от лиц, желающих получить доступ к корпоративным сетям или бизнес-приложениям. Управление методикой аутентификации пользователя осуществляется централизовано.

Сервер IDENTIKEY построен на основной платформе для систем аутентификации VACMAN разработки VASCO. Сервер обладает универсальностью и достаточно мощен для обеспечения высшей степени защиты в комплексе с удобными программными приложениями. Разработка сервера отвечает требованиям промышленных стандартов для передачи данных. Сервер пригоден для защиты как крупных, так и малых корпоративных сетей, приложений и банковских онлайн-каналов.

Сервер IDENTIKEY отлично приспособлен для работы с большинством инструментов удаленного доступа, например, SSL-VPN, межсетевыми устройствами защиты firewall, внутренними и внешними сетями, а также с различными веб-приложениями. Он отлично работает на платформе Windows или Linux без каких-либо проблем, характерных для обслуживания систем двухфакторной аутентификации.

Сервер IDENTIKEY считается надежным универсальным устройством, способным обеспечивать одновременный вход в систему от десятков до миллионов человек. Для крупных систем на случай отказа предусмотрено восстановление сервера и копирование баз данных.

Модернизация действующей инфраструктуры

Сервер IDENTIKEY эффективно интегрируется в любую среду RADIUS. Таким образом, клиент продолжает пользоваться своей действующей инфраструктурой. Интегрирование не влечет каких-либо дополнительных затрат, так как имеющаяся база данных и серверы не требуют замены. Хранение данных можно интегрировать в активные директории или в различные базы данных, совместимые с ODBC. IDENTIKEY взаимодействует с несколькими серверами аутентификации в среде RADIUS и способен обеспечивать поиск в формате открытого протокола LDAP по AD, ADAM и eDirectory.

Сервер IDENTIKEY разработан с учетом веб-функциональности. Сервер легко интегрируется в онлайн-приложения через протокол SOAP, что обеспечивает простоту модификации соединений с сервером без привлечения каких-либо дополнительных работ или ресурсов. Кроме прочего, сервер использует интерфейс управления с доступом через сеть и генерирует отчет о действиях пользователя в формате HTML или XML.

Простое управление

Сервер IDENTIKEY обладает несколькими характеристиками, значительно упрощающими работу администратора и помогающими сократить издержки. Все инструменты управления удобно помещены на едином интерфейсе. Доступ к такому инструменту централизованного управления осуществляется через Интернет-браузер из любой точки сети. Такая функция обеспечивает удаленное управление и предоставляет новые возможности провайдерам внешних услуг.

Сервер IDENTIKEY имеет расширенную функциональность составления отчетов, что позволяет генерировать полезные сводки пользовательской истории, работы с системами DIGIPASS и т.д. Такие отчеты в комплексе с функцией контроля безопасности способны обеспечить важную информацию для справочной службы и отчетности.

Легкая установка и запуск

Установку сервера IDENTIKEY сопровождает интуитивно понятный мастер установки. Быстрая автоматизированная установка позволяет приступить к работе практически моментально. Для этого потребуется лишь незначительное участие службы IT. Пользователи могут самостоятельно назначать свои устройства аутентификации DIGIPASS, обновлять пароли и изменять свои PIN-коды, не привлекая для этого справочную службу, что также сокращает затраты.

Сервер IDENTIKEY оборудован несколькими инструментами и имеет характеристики, обеспечивающие легкую установку, удобную регистрацию пользователя или перенос с установленных продуктов. В список таких функций включены перенос данных, динамическая регистрация пользователя, автоматическое заучивание пароля, управление массивами, автоматическое присвоение, а также множество других инструментов.

Добавление новых пользователей и/или приложений происходит так же просто, как приобретение лицензий. Встроенная автоматическая функция развертывания сокращает вмешательство справочной службы в работу системы. Программное обеспечение и устройства мобильной аутентификации готовы к использованию немедленно после поставки.

IDENTIKEY®

Высокая надежность

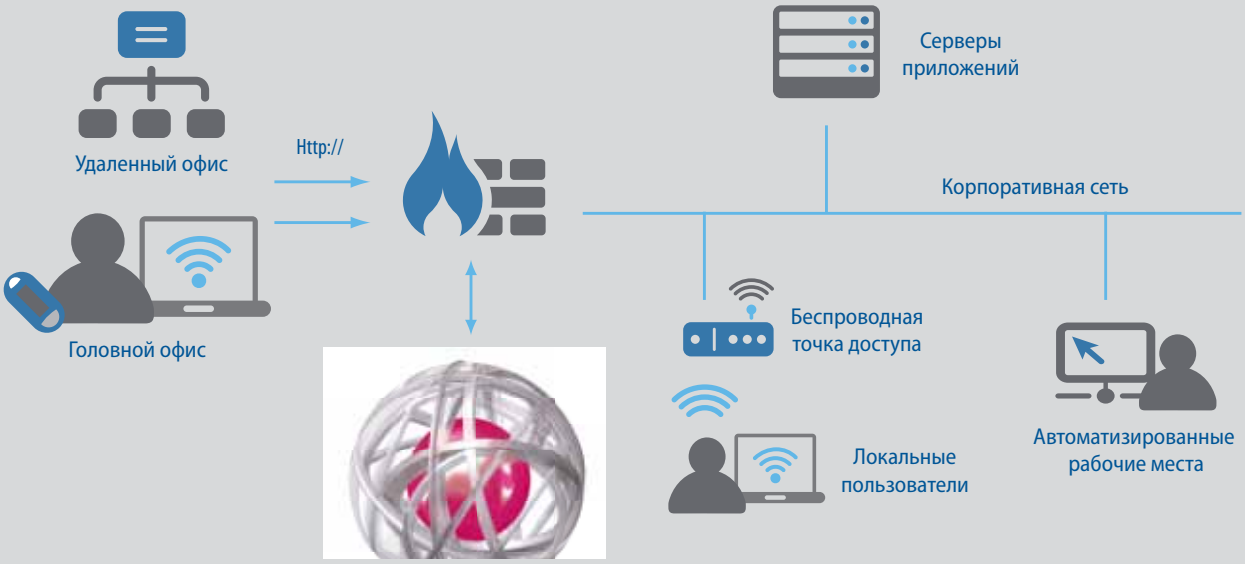
В целях бесперебойного обеспечения компания VASCO предусмотрела некоторые меры по защите от отказов, например, восстановление системы, резервирование и копирование баз данных. Сервер IDENTIKEY разработан с учетом расширения и наращивания производительности для масштабного развертывания.

Удобство пользователя

Система аутентификации на платформе IDENTIKEY не требует новых навыков работы пользователя или изменения IT-инфраструктуры. Несложный способ аутентификации всего лишь добавлен к существующим приложениям.

УСТРОЙСТВА DIGIPASS

Конечные пользователи сервера IDENTIKEY получают клиентское устройство DIGIPASS. В семейство продуктов DIGIPASS разработки VASCO включен широкий ряд устройств аутентификации конечного пользователя, предусмотренных для работы с IDENTIKEY. Клиент имеет возможность по своему усмотрению самостоятельно выбрать устройства аутентификации как программные (для браузера или мобильного телефона), так и аппаратные. Все устройства аутентификации DIGIPASS будут выполнены с учетом требований клиента, включая его логотипы и корпоративные цвета.



IDENTIKEY

Безопасный удаленный доступ для удаленных офисов и командированного персонала
Безопасный вход в локальную сеть через беспроводной узел доступа или настольный ПК на платформе Windows

ИДЕАЛЬНОЕ РЕШЕНИЕ ДЛЯ МАЛЫХ И СРЕДНИХ ПРЕДПРИЯТИЙ

IDENTIKEY представляет собой надежный и универсальный сервер аутентификации, рассчитанный на предприятия любого размера, включая малые и средние. Сервер обеспечивает высокую безопасность доступа к корпоративным сетям и местным приложениям. За счет дополнительного уровня защиты, предусмотренного для входа из сети Интернет, сервер IDENTIKEY обеспечивает безопасное соединение для персонала, работающего на дому, торговых представителей, командированных работников, удаленных офисов и бизнес-партнеров.

Сервер IDENTIKEY устанавливается на любом сервере. Интуитивная установка сопровождается инструкциями "мастера установки". Подключение к внешнему интерфейсу, например, защите firewall или маршрутизатору, а также к конечным серверам, осуществляющим дополнительный контроль статического пароля, выполняется автоматически. Вмешательство администратора ограничивается несколькими функциями: выбор местоположения сервера и хранение данных. Таким образом, сервер IDENTIKEY исключительно прост как в установке, так и настройке.

Сервер IDENTIKEY использует текущий стандарт обмена данными и совместим с широким перечнем наименований сетевого оборудования других изготовителей. Сервер легко интегрируется в действующую инфраструктуру.
По мере роста компании можно добавлять устройства конечных пользователей и приложения.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

- Поддержка среды RADIUS и веб-серверов
- Совместимость с большинством защитных программ firewall и серверами доступа
- Малый вес: простая установка, пользование и управление
- Поддержка баз данных, совместимых с ODBC
- Интеграция с сервисами активной директории
- Аутентификация на корпоративной платформе
- Объемная и автоматическая обработка
- Простота процедуры назначения устройств аутентификации DIGIPASS
- Динамическая регистрация пользователя
- Автоматическое заучивание пароля
- Система полного контроля и отчетности
- Интерфейс администратора с доступом через сеть
- Система управления на платформе Microsoft

Компания Qatargas

Qatargas действует на рынке сжиженного природного газа и является первопроходцем этой отрасли в эмирате Катар. Компания искала возможности обеспечения безопасности своих бизнес-приложений и сохранности данных для всех своих подразделений, а также возможности удаленного доступа к ним со стороны сотрудников и подрядчиков. Для защиты корпоративных сетей и приложений, а также для безопасного доступа высшего руководства, подрядчиков и удаленных офисов компании требовалось оптимальное решение, совместимое с платформой Citrix. Компания QatarGas остановила выбор на устройствах DIGIPASS разработки VASCO, что помогло повысить уровень безопасности удаленных сетей и бизнес-приложений за счет динамических паролей. Устройства DIGIPASS в комплексе с сервером IDENTIKEY могут быть размещены на платформе Citrix и, таким образом, обеспечивать безопасность удаленного доступа к метафрейму Citrix.

قطر للغاز
QATARGAS

БЕЗОПАСНЫЙ ОНЛАЙН-БАНКИНГ

Сервер IDENTIKEY является идеальным решением для банков, желающих внедрить систему надежной аутентификации без какого-либо значительного ущерба своему бюджету и ресурсам, либо для тех, кому не подходят крупные интеграционные проекты. Он также будет полезен банкам, которым необходим выделенный сервер для аутентификации. Имея в своем распоряжении сервер IDENTIKEY, финансовые организации могут предложить надежную аутентификацию в качестве дополнительного уровня защиты к перечню своих услуг: обслуживанию частных лиц, корпоративному обслуживанию, мобильному банкингу, информационно-справочной службе и т.д.

Сервер IDENTIKEY обеспечивает двухфакторную аутентификацию для клиентского доступа к приложениям онлайн-банкинга, а также функцию электронной подписи для подтверждения транзакции, являясь, таким образом, одним из наилучших решений на рынке по борьбе с MITM-атаками.

IDENTIKEY обладает способностью подтверждать динамические пароли для доступа к управлению и электронным подписям при проведении транзакций. С помощью таких инструментов как EMV-CAP и HSM, банки, действующие на развивающихся рынках, имеют комплексное решение по аутентификации, что полностью оправдывает их предыдущие инвестиции в системы аутентификации в инфраструктуре платежных карт. Наличие функции HSM в сервере IDENTIKEY обеспечивает оптимальную безопасность. В частности, ни при каких обстоятельствах шифроключи не будут раскрыты.

Сервер IDENTIKEY допускает конфигурацию в соответствии с требованиями провайдеров, которые, в свою очередь, могут предложить его своим клиентам как средство аутентификации. Пользуясь услугой аутентификации, банки могут избавить себя от части проблем в области безопасности, передав их своему партнеру, и сосредоточиться на основном бизнесе. Услуги провайдера оплачиваются на ежемесячной или ежеквартальной основе. Такой график является довольно привлекательным с точки зрения отчетности (обращение с наличностью, бюджетный контроль, управление инвестициями и т.д.).

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

- Помощь в борьбе с MITM-атаками
- Легко интегрируется в существующие банковские приложения
- К параметрам безопасности Интернет-банкинга добавлена надежная аутентификация и электронная подпись
- Быстрое размещение и пуск
- Полная функциональность (аутентификация, управление, отчетность, контроль, управление пользовательскими данными, управление устройствами DIGIPASS)
- Централизованная платформа аутентификации для нескольких сервисных центров (обслуживание частных и корпоративных лиц, мобильный банкинг и т.д.)
- Настраиваемая функциональность отчетности
- Обучение администраторов в рамках программы интеграции IDENTIKEY занимает всего несколько дней
- Поддержка модулей защиты EMV-CAP и аппаратного модуля безопасности (HSM)

IDENTIKEY ДЛЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В КАЧЕСТВЕ ОТДЕЛЬНОЙ УСЛУГИ

Идея размещения программного обеспечения претерпела некоторые изменения. В частности, традиционный подход, когда программы устанавливаются на отдельном компьютере, заменяется моделью, когда программное обеспечение и приложения предлагаются по запросу. Поставщики программного обеспечения в качестве отдельной услуги предлагают приложения на основе абонентской платы за пользование. При пользовании приложениями, размещенными на узле провайдера, администратора обычно беспокоят вопросы безопасности: как защитить учетные записи, защищена ли информация, переданная третьей стороне-провайдеру, обеспечен ли санкционированный доступ и т.д...

Компания VASCO нашла решение для безопасного доступа к приложениям за счет замены небезопасного статического пароля динамическим. Доступ к важной информации будет разрешен только авторизованным пользователям после подтверждения их подлинности. Эта мера исключает кражу данных и передачу учетных записей. Сервер IDENTIKEY можно связать с любым веб-приложением через протокол SOAP. Это будет надежной защитой для любого приложения в модели SaaS. Кроме прочего, сервер использует интерфейс управления с доступом через сеть и генерирует отчет о действиях пользователя в формате HTML или XML.

ПОСТАВЩИКАМ УСЛУГ

Сервер IDENTIKEY также рассчитан на пользование провайдерами управляемых услуг. IDENTIKEY моно разместить на узле сервисного партнера, который, в свою очередь, может предложить его клиентам в качестве услуги по аутентификации. Аутентификация как отдельно поставляемая услуга позволит компаниям сосредоточить силы на основном бизнесе, поручив аспекты безопасности подрядчику. Услуги провайдера оплачиваются на ежемесячной или ежеквартальной основе. Такой график является довольно привлекательным с точки зрения отчетности.

Сервер IDENTIKEY является отличным инструментом для запуска услуги по аутентификации:

- Готовое и универсальное серверное решение
- Запрос на аутентификацию для веб-приложений перенаправляется по протоколу SOAP через SSL на сервер IDENTIKEY, установленный у поставщика услуги. Запрос на аутентификацию, поступивший через стандартное оборудование RADIUS или внутренние веб-сайты, перенаправляется через виртуальную сеть VPN на тот же сервер IDENTIKEY.
- Различные авторизованные администраторы могут обслуживать несколько клиентов
- Счета клиенту выставляются на основе подробной отчетности

IDENTIKEY - НАДЕЖНАЯ ЗАЩИТА ПРЕДПРИЯТИЯ

Кроме защиты Интернет-приложений, сервер IDENTIKEY способен обеспечить безопасность удаленного доступа персонала к корпоративным сетям и ресурсам, для чего в конфигурации сервера предусмотрены различные расширения. Надомные работники, удаленные подразделения и офисы, командированный персонал и торговые представители могут пользоваться одной и той же технологией DIGIPASS для безопасного соединения через программы защиты виртуальных сетей firewall, SSL-VPN, или любое другое оборудование RADIUS с корпоративными сетями LAN для доступа к данным, документам или приложениям. Кроме того, за счет строгой аутентификации пользователя обеспечивается защита корпоративных порталов, почтового приложения Outlook Web Access и веб-приложений в интерфейсе Citrix.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

- Связь сервера IDENTIKEY с любым веб-приложением обеспечивается через интерфейс SOAP
- Благодаря серверу IDENTIKEY, поставщики услуг и средства информации используют различные учетные записи, что обеспечивает надежность структуры доходов
- Сервер IDENTIKEY обеспечивает нашим партнерам возможность предложить клиентам услуги по аутентификации
- Сервер IDENTIKEY обеспечивает наших партнеров платформой для аутентификации, позволяющей предлагать услуги независимого контроля и управления сразу нескольким клиентам
- Клиентская база данных может быть установлена на нескольких доменах с авторизованными администраторами
- Каждый счет сопровождается отдельной отчетностью

УСТРОЙСТВО АУТЕНТИФИКАЦИИ DIGIPASS ДЛЯ СРЕДЫ WINDOWS

Устройство аутентификации DIGIPASS для среды Windows в качестве расширения к серверу IDENTIKEY является экономически эффективным решением для предприятий, желающих защитить свои компьютеры на платформе Windows, подключенные к корпоративной сети, от несанкционированного доступа. Решение позволяет пользователям получать доступ к своим компьютерам с ОС Windows, подключенным к сети, с помощью динамического пароля (OTP), генерированного устройством DIGIPASS.

Устройство аутентификации DIGIPASS для среды Windows устанавливается в виде небольшого программного модуля на пользовательском компьютере. Устройство предусмотрено для установки как на настольных, так и переносных компьютерах, подключенных к корпоративной сети. Непосредственно после установки устройства аутентификации DIGIPASS для среды Windows обычное окно входа в систему будет заменено на версию, отсылающую учетные данные на сервер IDENTIKEY для проверки и подтверждения. После подтверждения запроса на аутентификацию оригинальный статический пароль отсылается обратно на компьютер и используется для входа в домен.

Если переносные компьютеры используются за пределами корпоративной сети, например, в пути или дома, модуль входа в систему будет работать в автономном режиме, обеспечивая те же функции надежной аутентификации, как и в подключенном режиме. Такая мера препятствует несанкционированному доступу, даже когда компьютер оставлен без надзора или в случае хищения переносного компьютера. Если компьютер работает в неподключенном режиме, учетные данные сверяются с локальной базой данных динамических паролей. Такие пароли генерируются, когда компьютер работает в подключенном режиме. Затем они надежно шифруются и сохраняются. Пользователь может работать в автономном режиме в течение несколько недель, используя заблаговременно генерированные динамические пароли.

IJZA

Организации по делам молодежи в Северном Брабанте (Нидерланды) разработали веб-приложения для эффективной регистрации контактных данных лиц, работающих в сфере защиты интересов молодежи. Поскольку информация, занесенная в базу данных приложения, носит исключительно конфиденциальный характер, организация IJZA искала надежный метод аутентификации для безопасного доступа к веб-приложениям. Главным условием была двухфакторная аутентификация. Другим условием была высокая мобильность, поскольку работа в сфере защиты интересов молодежи предполагает множество поездок. Следующим непременным условием был удаленный доступ к приложениям, так как их контроль осуществлялся непосредственно из организации. Таким образом, IJZA требовалось удобное и простое решение. Решение на основе сервера IDENTIKEY в комплексе с DIGIPASS соответствует всем этим условиям IJZA. Решение является мобильным и обеспечивает удаленный доступ. Кроме того, сервер IDENTIKEY имеет простой и удобный веб-интерфейс, позволяющий системным администраторам без труда управляться с процессом аутентификации.

ПАРТНЕРЫ И ВЫДЕЛЕННЫЕ МОДУЛИ

Для совместимости решений, предлагаемых другими поставщиками технологий, с решением VASCO DIGIPASS компания VASCO разработала партнерскую программу DIGIPASS Ready Partner Program. Теперь партнеры имеют возможность увязать свои решения с механизмом надежной аутентификации VASCO, либо разработать новые решения, в которые можно было бы интегрировать аутентификацию VASCO.

Выгода клиентов от простой и дешевой интеграции решений вполне очевидна. Они имеют возможность приумножить доходы от инвестиций, используя инфраструктуру для аутентификации, и устройства DIGIPASS, которые уже используются для множества задач.

Чтобы подробнее ознакомиться со списком партнеров VASCO, посетите страницу по адресу: www.vasco.com/solutions/partners

Выделенные модули

Для улучшения процесса интеграции сервера IDENTIKEY в пакете партнерских продуктов, специалисты VASCO разработали специальные выделенные модули. Такие плагины обеспечивают простую интеграцию устройств надежной аутентификации DIGIPASS в партнерские продукты. В конечном итоге, такое решение является экономичным и способствует повышению безопасности клиентской инфраструктуры удаленного доступа. Общий и подробный обзор поддерживаемых платформ можно найти по адресу www.vasco.com.

Готовые выделенные модули включают следующие:

Устройство аутентификации DIGIPASS для сервера Juniper SBR

Сервер Juniper Networks' Steel Belted RADIUS относится к семейству серверов RADIUS, использующих протокол AAA и разработанных для обеспечения безопасного доступа к сети. Сервер удовлетворяет требованиям большинства предприятий и поддерживает технологии доступа, банк пользовательской аутентификации и протоколы аутентификации. Компания VASCO разработала серверный модуль аутентификации IDENTIKEY Server DIGIPASS для SBR. Модуль легко настраивается и интегрируется в SBR. Модуль перенаправляет все запросы по аутентификации, поступающие на SBR, на сервер IDENTIKEY для дальнейшего подтверждения.

DIGIPASS Authentication для CA SiteMinder

Computer Associates' Siteminder является централизованной системой управления доступом к сетям Интернет, обеспечивающей аутентификацию пользователя, регистрацию, интеграцию идентификации и подтверждение пользовательских полномочий. Система позволяет предприятиям и крупным корпорациям управлять удаленным доступом в соответствии с корпоративными правилами и методами. Компания VASCO разработала серверный модуль аутентификации IDENTIKEY Server DIGIPASS для SiteMinder. Модуль легко настраивается и интегрируется в сервер SiteMinder. Модуль перенаправляет все запросы по аутентификации, поступающие на CA SiteMinder, на сервер IDENTIKEY для дальнейшего подтверждения.

Устройство аутентификации DIGIPASS для интерфейса Microsoft Outlook Web Access (OWA)

Outlook Web Access является веб-интерфейсом для Microsoft Exchange. Интерфейс обеспечивает мобильным или удаленным пользователям доступ к своим корпоративным почтовым системам через сеть Интернет. Для регистрации и входа в систему через MS Exchange по умолчанию используется тот же идентификатор пользователя и пароль, что и для центральной системы. Таким образом, слабая защита входа в систему практически открывает несанкционированный доступ к почтовым ящикам и другой конфиденциальной информации. Устройство аутентификации DIGIPASS для OWA позволяет заменить статические имя и пароль пользователя динамическим паролем (OTP).

Устройство аутентификации DIGIPASS для OWA легко устанавливается и интегрируется в Exchange без какого-либо дополнительного программирования. Программа не замещает и не изменяет основную функциональность MS Exchange или OWA. После установки программа собирает учетные данные и направляет запрос аутентификации на сервер IDENTIKEY. Действительное пользовательское имя и пароль после проверки вводятся в Outlook Web Access и MS Exchange для дальнейшего входа в систему. Модуль аутентификации DIGIPASS для Microsoft Outlook Web Access эффективно обеспечивает дополнительный уровень безопасности для удаленного входа через небезопасные сети.

Устройство аутентификации DIGIPASS для веб-интерфейса Citrix (CWI)

Система надежной аутентификации VASCO легко встраивается в интерфейс Citrix для программ XenApp и XenDesktop и не влияет на их функциональность. При вводе данных клиента сервер IDENTIKEY проверяет их достоверность. После проверки пользователю разрешается доступ ко всем разрешенным приложениям.
При непосредственной интеграции в веб-интерфейс для программы Citrix XenApp, новый процесс аутентификации становится прозрачным для конечного пользователя и не требует дополнительных шагов или новых экранов ввода данных.

Порядок входа в систему конечного пользователя остается прежним, а организация приобретает дополнительную защиту в виде двухфакторной аутентификации.

"

CITRIX

"По мере расширения платформы Citrix, стратегические партнеры будут иметь для нас все большее значение. Компания не прекращает поиск новых партнеров, способных дополнить ряд основных продуктов и преумножить доходы клиентов. Мы доверяем решениям VASCO. Наши продукты исключительно совместимы, вот почему мы с удовольствием работаем сообща".

Марк Б. Темплтон. президент и генеральный директор компании Citrix

"

ДОПОЛНИТЕЛЬНЫЕ ИНСТРУМЕНТЫ

Кроме возможностей и функциональности сервера IDENTIKEY, компания VASCO предусмотрела дополнительные инструменты, способствующие размещению, переносу, управлению и ежедневной эксплуатации сервера аутентификации в инфраструктуре систем безопасности.

Инструмент синхронизации по протоколу LDAP

Инструмент синхронизации по протоколу LDAP предусматривает синхронизацию всего списка учетных записей пользователя в хранилище данных IDENTIKEY с внутренней директорией LDAP в ручном, автоматическом или запланированном режиме. Инструмент синхронизации по протоколу LDAP сокращает задачи администратора, связанные с созданием, удалением или обновлением списка пользователей и присвоенных устройств DIGIPASS, так как эти задачи будут исполняться автоматически.
Поскольку база данных IDENTIKEY будет постоянно обновленной, вмешательство администратора или справочной службы будет сведено к минимуму, что также способствует окупаемости затрат.

Менеджер синхронизации паролей

Менеджер синхронизации паролей обеспечивает синхронизацию статического пароля пользователя в хранилище данных IDENTIKEY с паролем в активных директориях. Если пользователю по какой-либо причине необходимо обновить пароль в активных директориях, новый пароль будет автоматически копирован в базу данных IDENTIKEY, где он будет использоваться для подтверждения или воспроизведения в некоторых приложениях. Так как базы данных IDENTIKEY обновляются автоматически, вмешательство со стороны администратора или справочной службы сводится к минимуму, что также способствует окупаемости затрат.

Инструмент миграции данных

В сервере IDENTIKEY предусмотрен инструмент миграции данных для перемещения информации баз данных из одной версии ПО в другую, совместимую с IDENTIKEY. Инструмент позволяет клиентам, пользующимся более ранней версией программного обеспечения VASCO, например VACMAN Server, VACMAN Middleware или плагинами для сторонних приложений, без труда мигрировть пользовательскую базу данных, включая все устройства DIGIPASS, а также личную и историческую информацию, в базу данных IDENTIKEY.

Сервер IDENTIKEY - сервер аутентификации VASCO следующего поколения

Комплект DIGIPASS для удаленной аутентификации

Комплект DIGIPASS для удаленной аутентификации специально разработан для малых и средних предприятий. Он обеспечивает высокий уровень защиты важной информации и внутренних приложений при удаленном доступе, не влияя сколько-нибудь на удобство пользования. Комплект предназначен для организаций с ограниченным IT-ресурсом и бюджетом. Он имеет полную функциональность решений по аутентификации, выбранных для конкретной системы. Комплексное решение включает всё необходимое программно-аппаратное обеспечение для развертывания систем двухфакторной аутентификации, что позволяет клиенту подготовить и запустить систему всего за один день. Решение исключительно универсально и предусматривает добавление новых пользователей и приложений по мере необходимости.

Для генерирования динамического пароля ОТП конечному пользователю необходимо всего лишь нажать кнопку на устройстве аутентификации или активировать приложение на своем мобильном телефоне. Затем конечный пользователь вводит генерированный пароль вместе с PIN-кодом на экране входа в систему. Сервер IDENTIKEY проверяет и верифицирует запрос на аутентификацию и подтверждает данные, если они совпадают с динамическим паролем, генерированным на серверном узле. При каждом новом входе в систему будет генерироваться новый динамический пароль.

Комплект DIGIPASS для удаленной аутентификации ни при каких обстоятельствах не влияет на функциональность клиентской IT-инфраструктуры и приложения. Пакет совместим с большинством защитных программ firewall, с серверами удалённого доступа и всеми сетями VPN на платформе RADIUS. Программы поддерживаются более чем 200 провайдерами приложений. Комплект DIGIPASS рассчитан на использование с любым клиентом RADIUS. При этом, какие-либо программные требования отсутствуют. Решение по аутентификации работает на клиентском сервере и практически не требует установки программ и их поддержки. Требования наличия какого-либо клиентского программного обеспечения отсутствуют. Компании имеют возможность защитить свои сети VPN и SSL VPN без каких-либо системных изменений.

Комплект DIGIPASS для удаленной аутентификации является идеальным решением для:

- Удаленного доступа к внутренним сетям через программу защиты firewall или SSL VPN
- Персонала, пребывающего в командировке, надомных работников, удаленных офисов, бизнес-партнеров, консультантов и т.д.
- Для веб-приложений, таких как Citrix CWI, SharePoint или Webmail предусмотрено расширение внутренних и внешних сетей и корпоративных веб-приложений, например, OWA

Комплект DIGIPASS для удаленной аутентификации рассчитан на работу с сервером IDENTIKEY. Сервер проверяет запрос на аутентификацию и централизовано управляет методом аутентификации пользователя. Со своей стороны, клиент может выбрать либо DIGIPASS GO 6 - однокнопочное устройство аутентификации, генерирующее динамический пароль, либо DIGIPASS для мобильных телефонов - программу, встраиваемую в мобильный телефон для аутентификации.

aXsGUARD Identifier

aXsGUARD Identifier идеально подойдет для предприятий, которым необходимо выделенное устройство для аутентификации, и которые желают избавить себя от лишних хлопот, связанных с установкой и обслуживанием ПО. aXsGUARD Identifier является надежным средством аутентификации пользователя при местном или удаленном доступе к корпоративным сетям или веб-приложениям. aXsGUARD Identifier компактно выполнен, монтируется в 19-дюймовой стойке и полностью дублирует функциональность сервера IDENTIKEY.

Решение разработано для предприятий, не пожелавших совместно использовать единый серверный ресурс из-за множества важных рабочих приложений. Таким образом, им предоставляется выделенное устройство, позволяющее обрабатывать запросы на аутентификацию без каких-либо изменений в существующей IT-инфраструктуре. Для малых и средних предприятий, а также для крупных международных корпораций предусмотрено множество аппаратных версий. Выбор версии зависит от количества пользователей. Оборудование является взаимозаменяемым, обеспечивает безотказную работу и настройку рабочих параметров для каждого удаленного узла.

Предлагаются следующие аппаратные версии:

- Версия AG3442 разработана для малого бизнеса или малых удаленных узлов. Оборудование бесшумно, потребляет мало мощности, выполнено в корпусе 1U на 19-дюймовой стойке, но обладает всеми характеристиками и функциональностью IDENTIKEY и определителя.
- Версия AG5502 выполнена в корпусе 1U на 19-дюймовой стойке и рассчитана на работу с основными приложениями в любой бизнес-среде. Оборудование обеспечивает аутентификацию до 10 000 пользователей. Устройство идеально для обеспечения безопасного входа в сети VPN, Интернет и Windows на крупных предприятиях.
- Версия AG7552 представляет собой полностью резервированный сервер в корпусе 2U на 19-дюймовой стойке. Этот сервер с двухъядерным процессором, 12 ГБ RAM и жесткими дисками емкостью 1 ТБ в блоке RAID 1 является отличным решением для работы с важными бизнес-приложениями. Сервер можно также использовать в качестве контрольной или резервной системы на средних и крупных предприятиях.

Благодаря синхронизации с протоколом LDAP обработка информации пользователя осуществляется в основной корпоративной базе данных LDAP (Microsoft Active Directory, Novell e-Directory, или в любой другой директории LDAP). Такая характеристика позволяет повысить уровень безопасности и сократить участие администратора в обработке пользовательских данных.

aXsGUARD Identifier обладает функциональностью контроля и генерирования отчетов. Мониторинг входящих и текущих запросов на аутентификацию в среде RADIUS и Интернет осуществляется с контрольной панели. Статистическая отчетность позволяет администратору без труда управлять средой удаленного доступа, стандартными и специальными отчетами формата XML, а также вести расширенный поиск в журнале регистраций.

ПРЕИМУЩЕСТВА

- Простая установка и эксплуатация
- Интуитивный пользовательский интерфейс с "мастером подсказок", доступный через сеть
- Автоматическое обновление с механизмом абсолютной надёжности
- Функция выделенных задач позволяет назначать и присваивать задачи (пользователь, управление DIGIPASS, отчетность)
- Самостоятельная регистрация для конечного пользователя
- Удаленное или переданное третьим лицам администрирование
- Удаленная поддержка (на основании отдельного договора)

aXsGUARD®

ПРОФЕССИОНАЛЬНЫЕ УСЛУГИ VASCO

Внедрение систем двухфакторной аутентификации связано со многими аспектами. Служба профессиональных услуг VASCO создана для оказания клиентам поддержки в реализации проекта систем аутентификации. Делясь своим опытом, мы помогаем клиентам решить любые проблемы и достичь наилучшего результата, избавляя их от излишних хлопот на всем протяжении реализации проекта.

Реализация проекта двухфакторной аутентификации касается не только отдела информационной безопасности. Проект охватывает другие службы и отделы. Значит, для его реализации потребуется структурный подход и хорошо продуманное руководство проектом на всех этапах, включая логистику, маркетинг, информационную безопасность, развертывание, организацию службы справки и поддержки и т.д.

Наши специалисты позаботятся о следующем:

- Управление проектом аутентификации
- Консультации по выбору технологий
- Консультации по маркетинговой стратегии
- Запуск и внедрение приложения
- Управление логистикой и запасами
- Организация службы справки и поддержки

Наши специалисты используют 4-ступенчатую испытанную методику VASCO. Вместе с клиентом мы проходим все этапы, от определения цели модернизации систем безопасности, до готового результата, отвечающего особым требованиям клиента.

Компания VASCO предлагает ряд специальных профессиональных услуг, относящихся к проектам IDENTIKEY, включая следующие:

- Модуль крупных проектов сервера IDENTIKEY
- Комплекс работ по установке сервера IDENTIKEY
- Комплекс работ по интеграции сервера IDENTIKEY в систему
- Комплекс работ по обеспечению работы сервера IDENTIKEY

КОНСУЛЬТАЦИОННЫЕ УСЛУГИ VASCO

Консультационная служба является еще одной качественной услугой в перечне предложений VASCO. Служба рассчитана на поддержку клиента и консультации в области систем аутентификации.

Если требуется информация о текущих проблемах, связанных с безопасностью и угрозами в области электронного банкинга и коммерции или информационной безопасности, либо вам необходим правильный совет на этапе до и в ходе реализации проекта, можете рассчитывать на опыт и профессионализм специалистов VASCO.

Делясь опытом, наработками и методикой, компания VASCO помогает клиентам экономить время на осуществление проекта аутентификации.

Более подробно о наших консультационных услугах можно узнать по адресу: www.vasco.com/consulting

Академия специалистов по безопасности и электронная обучающая платформа VASCO (SEAL)

Новые типы онлайн-атак появляются практически ежедневно, поэтому для профессионалов, занятых в сфере информационной безопасности, очень важно оставаться информированными и быть в курсе последних событий. В качестве ведущего мирового поставщика решений в сфере Интернет-безопасности компания VASCO считает своим долгом активно делиться со своими клиентами, партнерами, посредниками, дистрибуторами и любым, кому требуется консультация, информацией о текущих и новых направлениях в области информационной защиты от мошеннических схем.

Программа SEAL, созданная по инициативе VASCO, является своеобразным мировым сообществом специалистов по безопасности. Программа обучения в рамках SEAL включает ряд тем, посвященных информационной безопасности, а также практическое обучение работе с продуктами VASCO, что значительно расширяет карьерные возможности специалистов, занятых в этой сфере. Обучение в рамках SEAL рассчитано на стационарные занятия в классах, удаленное обучение, курсы DVD или форумы. Клиентам и партнерам предоставляется возможность:

- Стать сертифицированным инженером VASCO
- Быть в курсе новейших направлений в области безопасности и защиты
- Приобрести новые навыки в области информационной безопасности
- Иметь доступ к обширному банку знаний сообщества специалистов по безопасности
- Обмениваться информацией с единомышленниками

За дополнительной информацией обращайтесь по адресу:
www.vasco.com/training

Помощь и поддержка

Техническая поддержка VASCO предлагается в виде нескольких специально разработанных предложений. Предусмотрен следующий план технической поддержки:

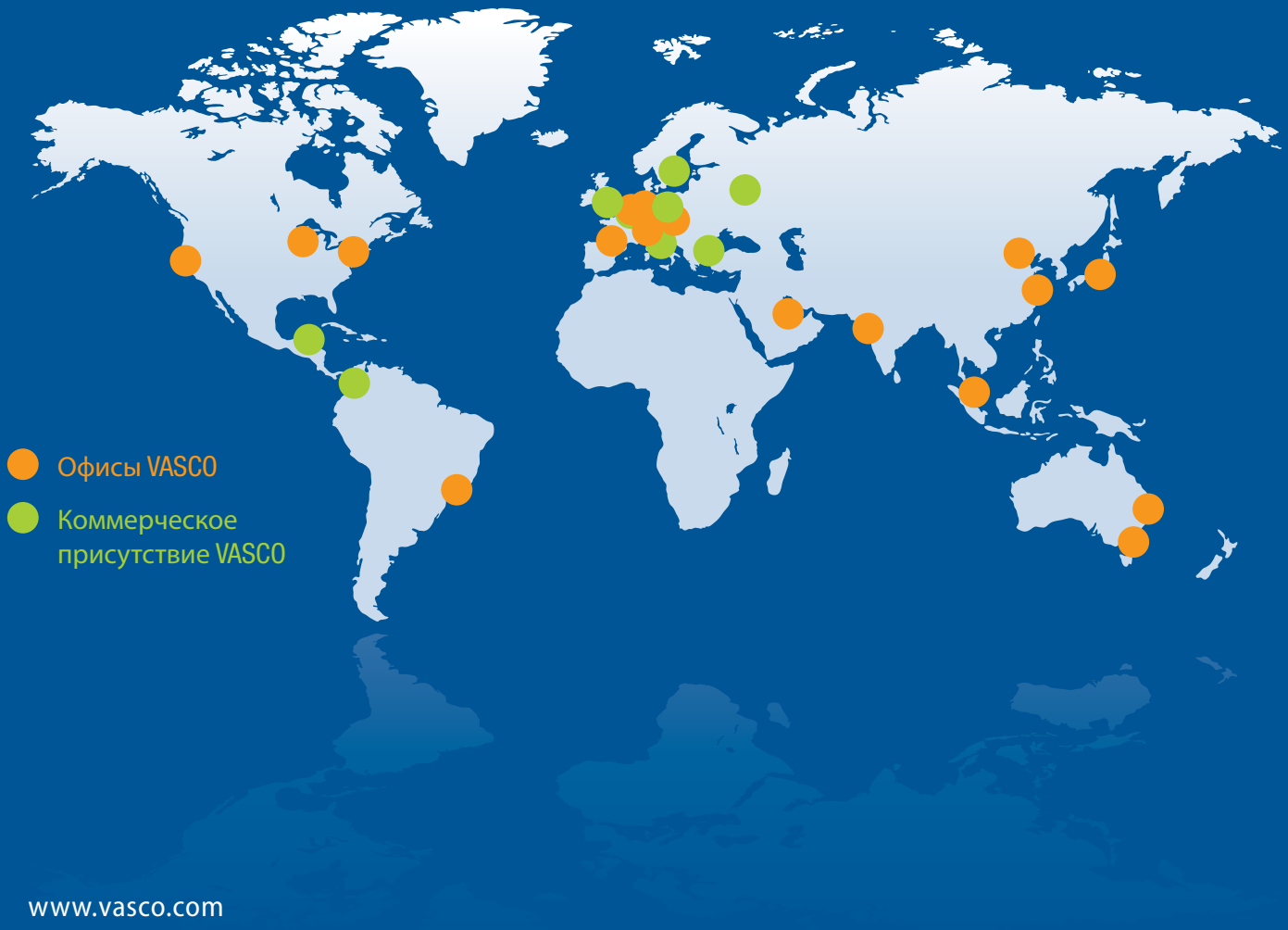
- Стандартная поддержка с понедельника по пятницу: время рабочее
- Круглосуточная поддержка формата 24/7
- VIP-поддержка: включает элементы стандартной поддержки и адаптирована под нужды конкретного клиента
- Поддержка с оплатой по факту
- Удаленное содействие

Более подробно о планах специальной поддержки можно узнать по адресу:
www.vasco.com/support

Сервер IDENTIKEY - сервер аутентификации VASCO следующего поколения

Компания VASCO

Компания VASCO является ведущим мировым поставщиком надежных решений в области аутентификации, цифровой электронной подписи, а также систем и приложений информационной безопасности. Компания позиционирует себя в качестве мирового разработчика систем безопасности в сети Интернет, обслуживая клиентов в более чем 100 странах, включая несколько международных финансовых организаций. К основным рынкам VASCO относится финансовый сектор, безопасность предприятий, электронная коммерция и электронный сектор правительственной документации.



www.vasco.com

МЕЖДУНАРОДНАЯ ШТАБ-КВАРТИРА
ЧИКАГО
Тел: +1.630.932.8844
email: info_usa@vasco.com

ОПЕРАТИВНАЯ ШТАБ-КВАРТИРА
БРЮССЕЛЬ
Тел: +32.2.609.97.00
email: info_europe@vasco.com

ШТАБ-КВАРТИРА
ФИНАНСОВОЙ СЛУЖБЫ
ЦЮРИХ
Тел: +41.43.555.3500
email: info_europe@vasco.com

ВАШ РЕГИОНАЛЬНЫЙ ОФИС

БОСТОН
Тел: +1.508.281.6670
email: info_usa@vasco.com

СИДНЕЙ
Тел: +61.2.8061.3700
email: info_australia@vasco.com

СИНГАПУР
Тел: +65.6323.0906
email: info_asia@vasco.com

Copyright © 2011 VASCO Data Security, Inc, VASCO Data Security International GmbH. Все права защищены. VASCO®, VACMAN®, IDENTIKEY®, aXsGUARD®, DIGIPASS® и логотип ® являются зарегистрированными торговыми марками компании VASCO Data Security, Inc. и/или VASCO Data Security International GmbH в США и других странах. VASCO Data Security, Inc. и/или VASCO Data Security International GmbH являются владельцами или держателями лицензии, собственности, прав, в том числе имущественных, на продукты VASCO, включая обновленные и измененные версии. Компании принадлежат авторские права, право на патент, коммерческую тайну, разработку шаблонов, баз данных и всю иную интеллектуальную и промышленную собственность в США и других странах. Microsoft и Windows являются торговыми марками или зарегистрированными товарными знаками корпорации Microsoft. Другие названия могут являться собственностью соответствующих владельцев.