ТЕХНИЧЕСКОЕ ОПИСАНИЕ

# Строгая аутентификация

## Как достичь требуемого уровня идентификации личности – удобно и экономично

### Краткий обзор

Непросто удовлетворить разнообразные потребности всех пользователей систем контроля доступа и при этом обеспечить защиту всех ресурсов от кибер угроз.

Чтобы доверять пользователям, предъявляющим свои личные данные, и эффективно управлять доступом к ресурсам, требуется комплексное решение для идентификации личности, основу которого составляет строгая аутентификация.

При этом выпуск и управление средствами идентификации пользователей на различных устройствах – от смарт-карт до поддерживаемых мобильных телефонов – для всех приложений и ресурсов, к которым пользователи желают получить доступ, могут поставить вас перед решением сложных задач. Таким образом, вам необходима надежная система аутентификации, которая позволяет легко выпускать средства идентификации и управлять ими, чтобы обеспечивать различные уровни безопасности в системе контроля доступа удобным для пользователя способом. Отсутствие строгой аутентификации снижает эффективность всего решения в целом.

## Содержание

## Необходимость строгой аутентификации в современных компаниях

По мере диверсификации, территориального распределения и повышения мобильности пользователей многие организации вынуждены пересмотреть свои концепции идентификации личности пользователей и контроля доступа. В прошлом основная защита располагалась по периметру предприятия, т.е. устройства физического контроля доступа размещались на входах в здание, а межсетевые экраны и виртуальные частные сети (VPN) ограничивали доступ к сети. Однако, получив доступ однажды, пользователи имели почти беспрепятственный доступ ко всем приложениям и ресурсам в зданиях и сетях.

На сегодняшний день остро стоит вопрос защиты от угроз «в собственных стенах». 81% компаний уже столкнулись с проблемой утечки данных вследствие халатности или умышленных действий сотрудников и других инсайдеров. Современный бизнес приобретает все более динамичный глобальный характер, разрушая привычные рамки, поэтому многие организации пересматривают свои концепции контроля доступа.

Наверняка и ваша компания из тех, которые стремятся максимально обеспечить потребности различных групп пользователей свести к минимуму риски, связанные с доступом этих пользователей к инфраструктуре предприятия. Эта задача усложняется тем, что виды угроз и количество пользователей непрерывно изменяются. Атаки становятся все более изощренными, о чем свидетельствует рост числа целенаправленных устойчивых угроз (APT, advanced persistent threat), использующих специальные вредоносные программы для длительных целевых атак. В то же время расширяется круг пользователей, которым требуется доступ к информации и ресурсам организации. Теперь это не только сотрудники, но и консультанты, подрядчики, производители, поставщики, партнеры и заказчики.

Все эти пользователи желают получать доступ из любой точки, где бы они ни находились, с помощью любых устройств, в том числе собственных мобильных телефонов, ноутбуков и планшетов (BYOD, концепция использования собственных устройств пользователей). Это может повысить риск для вашей инфраструктуры, если не принять меры предосторожности. Необходимо найти способ для идентификации личности всех различных групп пользователей, чтобы затем надлежащим образом контролировать доступ по мере перемещения этих пользователей по территории предприятия.

Применение принципов строгой аутентификации для каждого приложения является одним из наиболее эффективных способов повышения производительности вашей компании с одновременным снижением рисков. Обеспечивая защиту корпоративной инфраструктуры, облачных приложений и данных на ноутбуках и мобильных телефонах, вы можете эффективно управлять процессами контроля доступа и безопасностью ваших информационных ресурсов.

## Строгая аутентификация как способ решения задач, стоящих перед традиционными системами

Строгая аутентификация, также называемая расширенной или двухфакторной аутентификацией (AA), выходит за рамки простого ввода пароля. Для установления личности пользователя требуется проверка дополнительных факторов. Например, это может быть известная пользователю информация – уникальный пароль или персональный идентификационный номер (PIN-код), имеющееся у пользователя устройство – смарт-карта, токен или мобильный телефон, а также данные о попытках манипуляций и поведении пользователей, собираемые системой аутентификации.

Почему это так важно? Основной целью злоумышленников по-прежнему являются средства идентификации инсайдеров, так как с их помощью злоумышленники могут получить доступ к инфраструктуре и сетям предприятия и при этом незаметно передвигаться по территории компании. Проведенные недавно исследования показали, что причиной почти 50% случаев утечки данных стали похищенные или недостаточно защищенные средства идентификации. Учитывая эту статистику, очевидно, что повышение надежности аутентификации пользователей позволяет повысить общий уровень безопасности в организации.

Действительность такова, что применения традиционных статических паролей ввиду их удобства недостаточно для обеспечения защиты от современных динамических угроз, так как для взлома этих паролей могут использоваться программы регистрации нажатий клавиатуры, фишинговые атаки, перехват сообщений или простой перебор вариантов. Одноразовые пароли (OTP, one-time password) и токены обеспечивают повышенную защиту, поскольку генерируемые ими пароли действительны только для одной сессии или транзакции, однако их неправильная реализация может привести к новым проблемам. Во многих существующих системах невозможно контролировать цифровой идентификатор (сид) токена, который является «ключом» к данному токену. Как правило, сиды токенов хранятся в базах данных производителя, что означает угрозу безопасности вашего предприятия в случае утечки данных у этого производителя.

Кроме того, существующие системы, в которых после первичного контроля пользователь больше не рассматривается как угроза безопасности, не обладают достаточной гибкостью, чтобы учитывать роль пользователя, его местоположение и тип устройства в целях установления личности пользователя и предоставления доступа к широкому спектру ресурсов компании и облачных приложений. Недостаточно использовать строгую аутентификацию при первом входе в здание или сеть – как уже было сказано выше, проверка по периметру предприятия ушла в прошлое. Необходимо внедрить строгую аутентификацию в масштабе всей корпоративной инфраструктуры и включить в нее контроль доступа к данным и облачным приложениям на настольных ПК, серверах и мобильных телефонах, чтобы таким образом эффективно повысить общий уровень безопасности и контролируемости корпоративных ресурсов.

При этом выпуск и управление средствами идентификации пользователей на различных устройствах – от смарт-карт до мобильных телефонов – для всех приложений и ресурсов, к которым пользователи желают получить доступ, могут стать очень трудоемкими процессами. Дополнительную сложность представляет работа с несколькими типами средств идентификации для физического и логического контроля доступа, а также работа с различными системами аутентификации и выпуска средств идентификации. Здесь требуется единый процесс с использованием объединенной системы управления средствами идентификации пользователей, которая способна выдавать надежные средства идентификации для всех пользователей и назначать соответствующие права доступа к зданиям, облачным приложениям и прочим ресурсам с помощью различных форм-факторов: от смарт-карт до мобильных телефонов.

**ActivID Appliance – универсальность сразу**

- **Поддержка устройств:** смартфоны, планшеты, ноутбуки и т.д.
- **Способы аутентификации:** аппаратные и программные токены с одноразовым паролем, смарт-карты, идентификаторы устройств, адаптивная аутентификация, механизмы обнаружения манипуляций, внешние механизмы генерирования одноразовых паролей (по SMS или электронной почте) для аутентификации на уровне транзакций.
- **Приложения:** Windows, Salesforce.com, SAP, Oracle, Google и прочие облачные и бизнес-приложения.

## Требования, предъявляемые к эффективной строгой аутентификации. Никаких компромиссов

Эффективное решение строгой аутентификации должно повышать безопасность без существенных дополнительных затрат или роста сложности системы. В современных организациях только простые в обращении и управлении системы строгой аутентификации способны работать с множеством различных типов пользователей, чтобы обеспечивать защиту компании от большого числа известных и возможных в будущем угроз. Вам необходимо решение, обладающее перечисленными ниже характеристиками.

**Строгая аутентификация:**

- **Два фактора и более:** повышают надежность идентификации личности пользователя для выдачи ему соответствующих прав доступа.
- **Несколько уровней доступа:** на основе рисков, связанных с различными типами пользователей и транзакций. Необходимо предусмотреть прозрачные многоуровневые возможности для существенного повышения безопасности без снижения удобства для пользователей (как минимум для пользователей, использующих проверенные устройства и точки доступа). Для этого можно использовать решения, включающие в себя:
- **Расширенная защита от мошенничества:** при аутентификации пользователей можно учитывать такие факторы, как географическое положение и сведения об устройстве, чтобы таким образом ограничить доступ только для проверенных устройств в проверенных локациях.

Как вариант, пользователи могут использовать дополнительный, более надежный способ аутентификации (например, одноразовый пароль, отправленный в виде SMS), чтобы получить доступ с устройств или в странах, не входящих в проверенный список.

- **Непрерывный анализ поведения:** для текущей аутентификации и улучшения функций защиты от мошенничества на основе анализа поведения пользователя при работе с приложениями. Действия конкретного пользователя непрерывно контролируются и анализируются, чтобы в случае отклонений подавать сигнал тревоги. При этом сохраняется удобство для пользователя и конфиденциальность.

При обнаружении отклонения (например, другое лицо получило доступ к компьютеру) приложение может инициировать повторную аутентификацию пользователя и/или добавить событие в базу данных аудита с целью дальнейшего анализа возможного мошенничества. Данный метод позволяет сократить число шагов аутентификации, что удобнее для пользователя.

**Упрощенное управление:**

- **Быстрое внедрение и управление:** возможность настройки и запуска решения без существенных дополнительных затрат и роста сложности системы. В идеальном случае решение должно предоставлять вам единый интерфейс для упрощения выпуска средств идентификации и непрерывного управления системами по идентификации личности, чтобы гарантировать требуемый уровень безопасности (например, в нем должна иметься возможность простого распознавания и отзыва средств идентификации, чтобы деактивировать идентификатор сотрудника, покинувшего предприятие).
- **Наглядность:** единая система управления всеми средствами идентификации пользователей на различных устройствах (смарт-карты и мобильные телефоны) с возможностью непрерывного контроля этих средств идентификации и устройств. В идеальном случае система должна обеспечивать физический и логический контроль доступа (здания, облачные приложения и корпоративные ресурсы), предоставляя единый интерфейс со всеми системами идентификации личности.
- **Простая интеграция:** возможность интеграции решения в используемые системы обработки с целью создания единого интерфейса для управления средствами идентификации пользователей и аутентификацией.

**Удобство для пользователя:**

- **Простота в обращении:** решение не должно нарушать имеющиеся рабочие процессы. В идеальном случае оно должно использовать имеющиеся удостоверения личности, смарт-карты или мобильные телефоны пользователей, чтобы предоставлять расширенный доступ к физическим и сетевым ресурсам согласно требованиям пользователя.
- **Плавный переход:** решение не должно вызывать задержек в работе пользователей при доступе к корпоративным ресурсам и облачным приложениям.

## Решение для строгой аутентификации под требуемый уровень безопасности доступа

Ассортимент продукции ActivID™ предназначен для выпуска и управления средствами идентификации для различных типов пользователей, нуждающихся в доступе к вашей сети. При этом для удобной и безопасной аутентификации можно использовать любое устройство по желанию пользователя. Это мощное решение состоит из конвергированного средства идентификации ActivID, сервера аутентификации ActivID Appliance и системы управления картами ActivID CMS.

**Конвергированное средство идентификации:**

В ассортименте продукции ActivID представлено уникальное конвергированное средство идентификации, которое можно встраивать в смарт-карту, пропуск или даже мобильный телефон для использования в системах физического и логического контроля доступа. Таким образом, пользователи проходят процедуру аутентификации и получают доступ к зданиям, сетям, приложениям и прочим системам. Конвергированное средство идентификации также можно использовать для получения удаленного доступа к защищенным сетям, поэтому токены с одноразовым паролем или идентификационные брелки для ключа больше не требуются.

Конвергированное средство идентификации более удобно для пользователей, так как отсутствует необходимость носить с собой несколько устройств и повторно запрашивать одноразовые пароли. Оно также значительно повышает безопасность за счет строгой аутентификации во всей корпоративной ИТ-инфраструктуре (ключевые системы, сетевые ресурсы и облачные приложения), а не только по периметру.

**ActivID Appliance CMS:**

Возможность управления следующими компонентами:

- **Устройства аутентификации:** смарт-карты, USB-токены и мобильные телефоны.
- **Данные:** статические пароли, биометрические и демографические данные.
- **Апплеты:** микропрограммы для PIV (Personal Identity Verification) и генерации одноразовых паролей.
- **Цифровые средства идентификации:** в том числе сертификаты в инфраструктуре открытых ключей (PKI, Public Key Infrastructure) в течение всего жизненного цикла.

**Сервер аутентификации ActivID Appliance:**

Сервер аутентификации ActivID Appliance обладает необходимой универсальностью для эффективной и экономически выгодной реализации строгой аутентификации и защиты доступа пользователей к различным приложениям. Сервер поддерживает множество устройств и более 15 способов аутентификации, позволяя надежно устанавливать личность пользователей и предоставлять им доступ ко всем корпоративным ресурсам и облачным приложениям.

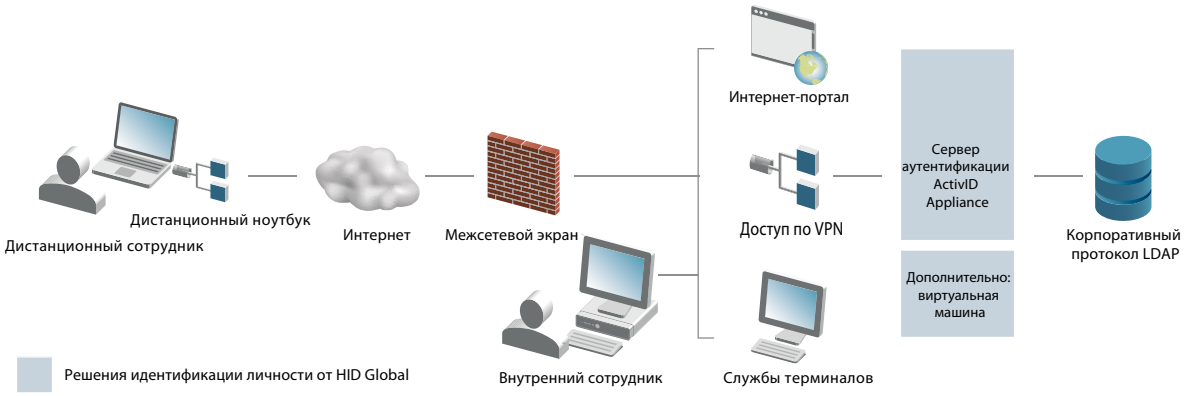
Сервер ActivID Appliance обеспечивает требуемый уровень безопасности без роста сложности системы. Используя шаблоны и просто задаваемые правила, можно быстро реализовать решение для строгой аутентификации в соответствии с конкретными потребностями. Уникальный сервис защиты от мошенничества на сервере ActivID Appliance позволяет настраивать систему в зависимости от особых требований вашей инфраструктуры. С его помощью можно регистрировать подробности доступа пользователей, например, с какого компьютера и веб-браузера осуществляется доступ и использовались ли они ранее. На основе этой информации можно принять решение о том, достаточно ли простой аутентификации или необходимо провести двухфакторную аутентификацию посредством заданного набора правил. Таким образом можно повышать безопасность простым для вас и незаметным для пользователя способом.

Вы можете индивидуально настраивать систему путем ограничения доступа к определенным устройствам в определенной зоне или путем проверки роли пользователя (генеральный директор или специалист по маркетингу), чтобы определить тип выдаваемого средства идентификации и способ контроля доступа. Вы также можете воспользоваться преимуществами информации, собранной тысячами других пользователей, чтобы при изменениях условий (например, в случае обнаружения отклонений в работе компьютеров в определенной зоне) можно было изменять требования к аутентификации (ограничение доступа или дополнительная аутентификация).

В результате, решение ActivID помогает вам идти в ногу с непрерывно изменяющимися требованиями и плавно интегрировать функции безопасности в рабочие процессы ваших пользователей, чтобы обеспечить дополнительную защиту для критичных ресурсов. ActivID помогает достичь соответствия с обновленными нормативами FFIEC, PCI DSS и прочими международными положениями, правилами и директивами для электронной коммерции и дистанционного банковского обслуживания. Срок службы токенов ActivID - до восьми лет, при этом вы сможете управлять цифровыми идентификаторами (сидами) своих токенов, сохраняя полный контроль за целостностью криптографических ключей.

При необходимости предлагаются профессиональные услуги HID Global для тонкой настройки сервиса защиты от мошенничества на сервере ActivID Appliance. Благодаря нашим услугам вы сможете разработать оптимальные правила для вашей инфраструктуры, учитывающие более 20 различных параметров: роли пользователей, время и место доступа, тип устройства и т.д. Таким образом можно просто и быстро ввести решение в эксплуатацию.

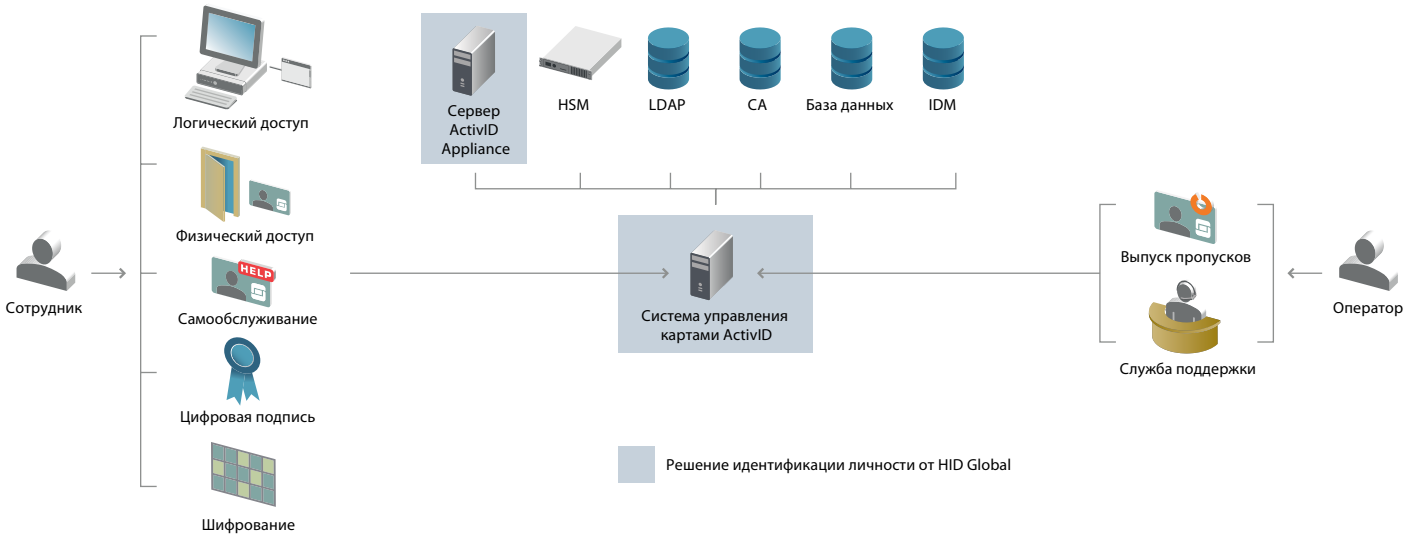
## Аутентификация ActivID Appliance: принцип работы




## Система управления картами ActivID

Система ActivID CMS представляет собой комплексное и универсальное решение для удобного управления процессами выпуска обслуживания смарт-карт, PKI-токенов (в т.ч. в мобильных телефонах), которые могут быть использованы для защиты доступа к рабочим станциям, сетевым ресурсам и корпоративным приложениям. Таким образом можно создавать индивидуальные рабочие процессы и правила, согласованные с вашей инфраструктурой и всеми сценариями развертывания. Система предоставляет полный, защищенный от манипуляций набор функций для регистрации всех событий и составления отчетов. Уникальный запатентованный механизм обновления после выпуска позволяет поддерживать вашу систему аутентификации в работоспособном состоянии. Веб-сервисы сервисы поддержки и самообслуживания помогают сократить эксплуатационные расходы, связанные с непрерывным обслуживанием системы.

## Система управления картами ActivID-CMS: принцип работы




## Как воспользоваться преимуществами эффективного решения для строгой аутентификации

Комплексное решение для строгой аутентификации ActivID CMS позволяет повысить уровень безопасности для различных групп пользователей в распределенной инфраструктуре. Благодаря универсальности решения можно сбалансировать затраты и требования по безопасности, чтобы предоставить пользователям удобный интерфейс и снизить риски, связанные с постоянно изменяемыми видами угроз.

**Строгая аутентификация:**

- **Снижение рисков:** защищенное соединение между пользователями и приложениями за счет аутентификации на основе двух или более факторов; защита от утечки данных.
- **Обнаружение мошенничества и анализ поведения пользователей:** предоставляют дополнительные факторы в процессе аутентификации, позволяющие повысить надежность идентификации пользователя, уверенность в безопасности доступа и удобство для пользователя.
- Стратегия адаптивной аутентификации: возможность определения различных уровней доступа, для правильного выбора выдаваемого средства идентификации (устройства) и способа контроля доступа для конкретного пользователя.

**Упрощенное управление:**

- **Быстрое внедрение и управление:** пользователи могут быстро начать работу в системе, используя токены для защиты доступа к приложениям в масштабе всей компании.
  - По мере роста потребностей организации можно легко обновить лицензию, чтобы получить доступ к широкому спектру способов аутентификации, включая решения на основе сертификатов, секретных вопросов и анализа рисков.
  - Решение включает в себя легко задаваемые политики безопасности и рабочие процессы для выпуска и управления цифровыми средствами идентификации и устройствами среди неограниченного числа групп пользователей в условиях географического распределения.
- **Сокращение затрат:** единое конвергированное средство идентификации устраняет необходимость в применении отдельных систем физического и логического контроля доступа. Оно упрощает процессы, сокращает бумажный документооборот и оптимизирует все процессы управления решением надежной идентификации личности.
  - Расширение возможностей карты доступа или мобильного телефона пользователя. Не требуются пароли и любые операции по сбросу пароля и пр.
  - Универсальная многоуровневая платформа аутентификации позволяет свести к минимуму денежные и временные затраты на внедрение и поддержку цифровых средств идентификации в виде смарт-карт, USB-токенов и мобильных телефонов.
  - Возможность уделять особое внимание безопасности определенных пользователей и приложений.
- **Расширенная функциональность:** наглядная, масштабируемая и конфигурируемая платформа для управления многофункциональными пропусками сотрудников, цифровыми идентификаторами на смарт-картах и токенами на мобильных телефонах.
  - Защита доступа к сетям VPN, Интернет-порталам и облачным приложениям с помощью смартфонов, планшетов, ноутбуков и ПК.
  - Простота интеграции с целым рядом операционных систем, служб каталогов, внешних и внутренних систем управления и контроля, центров сертификации и систем физического контроля доступа.
  - Полная совместимость со стандартом открытой аутентификации (OATH), расширение набора поддерживаемых устройств аутентификации.

**Удобство для пользователя:**

- **Простота в использовании:** бейдж или даже мобильный телефон пользователя можно использовать для физического и логического доступа. Простая интеграция в существующие рабочие процессы- не надо ничего лишнего носить или запоминать.

**Повышение производительности:**

- Невидимые меры безопасности, такие как обнаружение мошенничества и анализ поведения пользователя, позволяют сократить число шагов аутентификации, что повышает удобство для пользователя.
- Строгие политики безопасности на основе уровня риска и влияния на деятельность компании. Любые дополнительные меры только по необходимости (большое количество факторов: местоположение, тип устройства, роль пользователя, время, изменения в поведении и т.д.).

## ActivID – уверенность для пользователей и организаций

В современных динамических условиях только простое в обращении и управлении решение надежной аутентификации способно удовлетворить требования пользователей и организаций. Решение ActivID обладает необходимой универсальностью и надежностью для поддержки большого числа пользователей, которые используют множество различных устройств для доступа к широкому спектру ресурсов и корпоративных приложений. Оно применяется во многих организациях с повышенными требованиями к безопасности – от Министерства обороны до финансовых институтов и здравоохранительных учреждений. Как единственный поставщик полностью конвергированных систем контроля доступа, компания HID Global предлагает наиболее комплексное решение для идентификации личности, которое содержит все необходимые компоненты: от дверного считывателя пропусков до аппаратных и программных средств аутентификации. Внедрение этого решения позволяет повысить надежность идентификации пользователей и обеспечить эффективную защиту компании от текущих и будущих угроз. В результате пользователи могут устанавливать защищенное соединение из любой точки, используя разнообразные устройства и методы аутентификации, чтобы удобным для них способом получать все необходимые ресурсы для успешной работы во благо своей компании.

## О компании HID Global

Компания HID Global – это надежный поставщик инновационных продуктов, услуг, решений и технологий в сфере выпуска, использования и управления средствами идентификации для миллионов заказчиков по всему миру. Компания разрабатывает системы физического и логического контроля доступа, включая механизмы строгой аутентификации и управления средствами идентификации, а также решения для печати и персонализации карт, системы регистрации посетителей, высоконадежные правительственные и гражданские удостоверения личности, технологии радиочастотных меток для идентификации животных и применения в промышленности и логистике. Ведущие марки: ActivId®, EasyLobby®, FARGO® и HID®. Компания HID Global, главный офис которой расположен в г. Ирвин в Калифорнии, имеет более 2000 сотрудников по всему миру и международные представительства, работающие с более чем 100 странами. Компания HID Global® входит в состав ASSA ABLOY Group. Более подробная информация представлена на сайте **www.hidglobal.com.**



2014-02-24-hid-strongauthentication-wp-ru PLT-01897