WHITE PAPER

Конвергенция информационной безопасности и управления физическим доступом

Использование единой карты для доступа к ИТ и физическим ресурсам

Пояснительная записка

Организации все чаще применяют модель, предусматривающую использование одной карты или смартфона для различных ситуаций и профилей управления доступом. Подобная конвергенция ситуаций и профилей использования устраняет необходимость запоминать и иметь при себе несколько карт или других устройств для открытия дверей, входа в компьютерные системы и доступа к облачным приложениям, одновременно позволяя добавить в набор функций другие ценные приложения, включая безналичные расчеты, время и посещаемость или управление аутентификацией печати.

Существует растущий спрос на привязку всех средств доступа системой контроля ИТ и физических ресурсов к единой карте или смартфону, с помощью единого пакета процессов. Помимо очевидного удобства, конвергенция средств доступа на единой карте или устройстве способна значительно повысить безопасность и снизить текущие операционные расходы. Подобный метод также позволяет централизовать управление профилем и доступом, консолидировать задачи и быстро и эффективно использовать мощную аутентификацию по всей инфраструктуре организации для защиты доступа ко всем ключевым физическим и ИТ-ресурсам.

Новая интегрированная модель управления картами уводит организации далеко вперед сразу по четырем важнейшим направлениям: от карт до смартфонов; от устройств чтения до удобства доступа по прикосновению «tap-in»; от инфраструктуры открытых ключей (PKI, Public Key Infrastructure) до упрощенных решений с повышенной безопасностью и от уже существующих PKI до действительно единого управления доступом с сильной аутентификацией.

В данном техническом описании рассматриваются движущие механизмы, проблемы, варианты развертывания и результаты, связанные с применением комплексного решения управления доступом ИТ и физическими ресурсами, а также описывается ценность беспроблемного пользовательского опыта в работе с облачными приложениями и услугами, в процессе доступа к данным и открывания дверей. Здесь также поясняются преимущества унифицированных регистрационных и рабочих процессов, охватывающих множество профилей нескольких приложений ИТ безопасности и PACS.

Движущие механизмы конвергенции

Исторически организации концентрировались на создании надежного периметра по защите доступа к своим физическим и ИТ-ресурсам. Методы традиционного контроля доступа зависят от предоставления пользователем удостоверения личности для получения доступа в здание, а затем, после попадания внутрь, использования статических паролей для аутентификации при доступе к ИТ-ресурсам. Однако, учитывая природу современных Целенаправленных устойчивых угроз (APT) и все внутренние риски, связанные с вариантом использования собственных устройств (BYOD), эти методы по обеспечению надежности доступа являются недостаточными.

Организации требуют повышенной способности контроля доступа и использования сильной аутентификации по всей инфраструктуре, в качестве одного из уровней многоуровневой стратегии защиты. К сожалению, выбор эффективной и сильной аутентификации для защиты

фирменных данных традиционно является нелегкой задачей. Большинство доступных решений неадекватны либо с точки зрения возможностей защиты, либо с точки зрения стоимости и вызываемых ими трудностей или же неприемлемы как не обеспечивающие должного удобства для пользователя.

Сотрудников привлекает удобство возможности пользоваться единой картой или механизмом для быстрого и простого доступа к ресурсам, необходимым для ведения бизнеса. С этой целью организации должны реализовать решение, позволяющее защитить доступ ко всему — от двери корпоративной серверной до данных, программ и облачных приложений. Подобное решение должно сочетать в себе традиционно разделяемые области физической и ИТ безопасности для координации управления профилями и доступом пользователей организации.

Важность комплексного управления доступом

Действительно комплексное управление доступом включает одну политику безопасности, одно средство доступа и один журнал аудита. В некоторых организациях управление пользователем уже является полностью комплексным, то есть использующим единую корпоративную политику, определяющую допустимый доступ и использование ресурсов, единый архив администратора и единый инструмент ведения журнала для упрощения отчетности и аудита. Подобное решение позволяет предприятиям:

Удобство: заменяет токены с одноразовым паролем (OTP) или идентификационные брелки для ключа, устраняя необходимость ношения нескольких устройств или перепрограммирования OTP для получения доступа ко всем необходимым физическим или ИТ-ресурсам
Безопасность: обеспечивает сильную аутентификацию по всей ИТ-инфраструктуре ключевых систем и приложений (а не только по периметру), и даже на уровне двери,

Снижение расходов: устраняет необходимость инвестирования в несколько решений доступа, централизуя управление и консолидируя задачи в единый набор процессов администрирования и службы поддержки по выпуску, замене и отзыву средств доступа.

Рассматривая несколько вариантов реализации

В случае с моделью комплексного управления доступом средство доступа может существовать в самых различных видах, включая смарт-карту (напр., удостоверение личности) или даже смартфон. В зависимости от требований предприятия и существующей инфраструктуры, существует несколько вариантов архитектуры решения. Ниже приведены три наиболее распространенные модели:

- **Традиционная бесконтактная:**

Позволяет расширить существующую карточную систему физического доступа с помощью таких технологий как ¡CLASS®, ¡CLASS Seos® MIFARE™ и MIFARE DESFire™ для аутентификации на уровне сетей и приложений компании. Программы разворачиваются на рабочем компьютере пользователя, а бесконтактное считывающее устройство подключается к

нему или встраивается в него. Карта может «считываться» без физического контакта со считывающим устройством. Это удобно для пользователей, которые могут сохранить карту, ранее

со считывающим устройством двери, прикасаясь ею к компьютеру или ноутбуку для получения доступа к компьютеру, корпоративным и облачным приложениям.

В данном подходе не применяются PKI, связывающие открытые ключи с профилями пользователя через центр сертификации (CA). Используемые в федеральном пространстве, PKI с сильной идентификацией являются ключевым элементом логического доступа и цифрового подписания документов для агентств и их подрядчиков. Цифровой сертификат, включающий открытый ключ пользователя, помещается на карту аутентификация личности (PIV), в которой применяются технологии смарт-карты и биометрические характеристики (образец отпечатка с цифровой подписью), и которая также поддерживает методы многофакторной аутентификации. Вместо общего секретного ключа аутентификации здесь используется пара из открытого и личного ключей, которые объединены таким образом, что информация, обрабатываемая одним ключом, может быть декодирована только с помощью другого ключа. «Федеральный мостовой» используется для установления доверия между кросс-сертифицированными PKI агентств (т. е. отдельными и независимыми инфраструктурами, каждая из которых имеет свой корневой центр сертификации), таким образом обеспечивая безопасны обмен информацией о цифровых подписях и сертификатах, отправляемых из различных других государственных организаций-участников.

Традиционный бесконтактный подход устраняет множество проблем с управлением ключами PKI, но при этом поддерживает более ограниченный ассортимент случаев использования и не обеспечивает нужный уровень безопасности по сравнению с решениями на основе PKI. Бесконтактная не-PKI модель применяется в больницах, школах и других учреждениях, где с достаточно быстрой сменяемостью различным пользователям требуется доступ к одним и тем же ресурсам. Он также используется в качестве переходного решения там, где мандаты, например, Системы информации уголовного судопроизводства (CJIS), требуют защиты рабочих компьютеров и приложений сильной аутентификацией.

- **Двойная чип-карта:** Содержит бесконтактный чип для физического доступа и контактный чип для контроля логического доступа на единой смарт-карте. Такие средства доступа, как PKI-сертификаты и OTP-ключи, могут управляться контактным чипом с помощью системы обработки карт (CMS).

Модель двойной чип-карты популярна в средних и крупных предприятиях, работающих с секретной интеллектуальной собственностью (IP) или данными клиентов в сети, поскольку она обеспечивает надежный уровень безопасности. Она также позволяет предприятию упростить управление другими аспектами ИТ-безопасности и воспользоваться преимуществами уже выполненных инвестиций в PACS, поскольку, в большинстве случаев, CMS можно интегрировать непосредственно в систему упарвления PACS (часто называемую центральной системой PACS).

- **Чип-карты с двойным интерфейсом**: Используют преимущества единого PKI-совместимого чипа, с контактным и бесконтактным интерфейсом для поддержки управления физическим и логическим доступом. Данная карта может использоваться для поддержки контактного считывателя карт для случаев логического доступа, например, входа в компьютерную систему или подписи e-mail, и для PKI-аутентификации при физическом доступе.

Модель карты с двойным интерфейсом в первую очередь применяется федеральными правительственными организациями США, где мандат OMB-11-11 требует использования для физического доступа PIV-карт, указанных в стандарте FIPS 201. По умолчанию использование PKI по бесконтаткному интерфейсу может замедлять физический доступ. Для решения этой проблемы ожидается, что FIPS 201-2 позволит использовать пакет Открытый протокол для идентификации управления доступом и конфиденциального документирования (Open Protocol for Access Control Identification and Ticketing with privacY — OPACITY) для аутентификации и ключевых протоколов реализации соглашений, что примерно вчетверо увеличит эффективность критически важных задач. Это также позволит реализовать надежные беспроводные соединения, обеспечивающие использование PIN и биометрической информации в бесконтактном интерфейсе. А это, в свою очередь, еще больше усилит аутентификацию контроля как физического, так и логического доступа.

Сильная аутентификация у двери

Важным преимуществом конвергенции является предоставляемая ею организациям возможность использовать уже выполненные инвестиции в средства доступа для создания полностью операционно-совместимой многоуровневой системы безопасности для всех сетей, систем и дверей компании. Сильная аутентификация будет все больше использоваться не только для удаленного доступа, но и на рабочих компьютерах, в ключевых

приложениях, серверах, облачных системах и для доступа в помещения. Такое явление требует реализации сильной аутентификация у двери.

Первым из таких аспектов является федеральное пространство с существующими PIV--картами пользователей. При использовании PIV-карты на входе в здание цифровые сертификаты PIV-карты сравниваются со списком отзыва сертификатов (CRL, Certificate Revocation List), предоставляемым сертифицирующими органами. PKI-аутентификация является высокоэффективным и хорошо совместимым методом не только контроля логического доступа для защиты данных, но и контроля физического доступа для защиты помещений, последний из которых именуется «PKI у двери».

Агентства обычно применяют поэтапный подход к внедрению PKI у двери, по мере наличия бюджетных средств. Для обеспечения такой возможности они конфигурируют свою инфраструктуру таким образом, чтобы ее можно было легко и быстро обновить до сильной аутентификации PKI для контроля физического доступа, по мере готовности. Например, сначала всех владельцев карт PIV регистрируют в центральной системе, а затем, в соответствии с требованиями Управления служб общего назначения США (GSA), просто внедряют переходные считыватели, которые считывают уникальный идентификатор с карты и сопоставляют его с зарегистрированным владельцем карты без применения каких-либо техник аутентификации по стандарту FIPS-201. Такие переходные считывающие устройства в дальнейшем могут быть перенастроены на месте с целью поддержки многофакторной аутентификации.
Ожидается, что «PKI у двери» получит более широкое распространение по мере развития FIPS 201 и появления большего числа поддерживающих его продуктов. Также предвидится появление значительных возможностей для внедрения «PKI у двери» по сниженной стоимости для карт CIV (коммерческая аутентификация), технически аналогичных PIV-картам, но не подверженных дополнительным требованиям, связанным с использованием федеральным правительством, В отличие от федеральных агентств, пользователи CIV-карт не должны приобретать сертификаты в «точках доверия» или осуществлять ежегодные взносы за обслуживание, но сами могут генерировать собственные сертификаты. Несмотря на некоторое повышение стоимости карт в связи с размещением дополнительной памяти для хранения сертификатов, подобные незначительные расходы обеспечат ценные дополнительные преимущества более сильной аутентификации у двери. Подумайте, например, о муниципальном аэропорте, который сможет использовать CIV-карты параллельно с подобными PIV-картами, уже используемыми здесь сотрудниками федерального Управления транспортной безопасности (TSA) США. Руководство аэропорта сможет создать единую систему контроля доступа, поддерживающую как сотрудников аэропорта, так и работающие здесь федеральные службы, обеспечив тем самым повышенную безопасность путем усиления аутентификации.

Распространение сильной аутентификации на контроль инфраструктур физического и логического доступа также станет важным этапом для развития предприятия. Организациям требуется целый ряд методов аутентификации и гибкость в простоте поддержки различных пользователей и надлежащей защиты различных ресурсов. Благодаря простым в использовании решениям, предприятия могут обеспечить безопасность доступа, как с контролируемых, так и с неконтролируемых устройств, ко всем своим ресурсам. Не будучи вынужденными создавать или поддерживать множество инфраструктур аутентификации, предприятия смогут использовать единое решение для обеспечения безопасности доступа ко всем ресурсам, от двери в охраняемое помещение или копировального аппарата до виртуальных частных сетей (VPN), терминальных служб и облачных приложений.

А как же мобильные?

Как известно, пользователи становятся все более мобильными и все чаще для доступа к нужным им ресурсам в среде организации пользуются собственными устройствами (BYOD)

— смартфонами, ноутбуками и планшетами. Согласно данным ABI, к 2015 году в сети будет более 7 млрд. новых беспроводных устройства, что приближает нас к показателю одного мобильного устройства на человека на планете.

Организации стараются поддерживать подобный мобильный доступ, одновременно рассматривая варианты использования преимуществ мобильных устройств пользователей в качестве платформ для средств физического и логического доступа. При этом всегда существуют пилотные проекты, как например, проект Arizona State University, подтвердивший реальность концепции использования мобильного телефона как базы для средства физического доступа. Федеральное правительство также посматривает в сторону мобильного контроля доступа. Ожидается, что FIPS-201-2 будут включать такие расширения, как концепция вторичных средств идентификации, которые могут размещаться в элементе безопасности (SE) телефона с помощью тех же криптографических услуг, которые применяются и в карте.

Мобильный контроль доступа требует переосмысления способа управления средствами физического доступа, и превращения их в портативные, для смартфонов, что позволит организациям использовать смарт-карты или мобильные устройства, или и то, и другое в рамках их решений PACS. С этой целью HID Global создала новую модель для платформы iCLASS SE® под названием Secure Identity Object® (SIO®), способную представлять множество форм идентификационной информации на любом устройстве, активированном для работы в границах безопасности и центральной экосистемы управления идентификацией платформой Trusted Identity Platform® (TIP) компании. TIP использует канал безопасной связи для передачи идентификационной информации между проверенными телефонами, их SE и другими безопасными носителями и устройствами. Комбинация платформы TIP и объектов SIO не только повышает уровень безопасности, но и позволяет адаптировать систему к будущим требованиям (например, добавление новых приложений в идентификационную карту). Такая комбинация разработана для обеспечения особо надежной безопасности, и является особенно привлекательной в среде BYOD.

Модель контроля мобильного доступа позволяет поддерживать любые виды данных контроля доступа на смартфоне, включая данные для контроля доступа, безналичную оплату, биометрическую проверку, доступ к ПК и многие другие задачи. Средство аутентификации хранится на элементе безопасности мобильного устройства, а облачная модель предоставления идентификации устраняет риск копирования средства доступа, одновременно облегчая предоставления временного средства доступа, отмены утерянных или украденных карт, а, при необходимости, и контроля и модификации параметров безопасности.

Пользователи получают возможность иметь при себе целый ряд карт управления доступом, а также OTP-токена для входа в компьютерную систему, на телефоне, с помощью которого они могут пройти аутентификацию в сети, просто прикоснувшись им к персональному планшету. Сочетание мобильных токенов на телефоне с возможностями однократной регистрации в облачных приложениях позволяет объединить классическую двухфакторную аутентификацию с оптимизированным доступом к различным облачным приложениям на едином устройстве, которое пользователи редко забывают или теряют. Кроме того, тот же телефон может использоваться для открывания дверей и множества других применений.

Здесь также есть свои трудности, связанные с тем, что телефоны и мобильные устройства, используемые для приложений контроля физического и логического доступа, не принадлежать организации. Например, после окончания студентом университета, он/она не сдает свой телефон так, как это сделали бы сотрудники со своими картами при уходе из компании. Здесь критичным является вопрос личной конфиденциальности пользователей BYOD одновременно с защитой данных и ресурсов предприятия. Отделы ИТ гораздо меньше контролируют BYOD или потенциально опасные персональные приложения, которые могут быть установлены на этих устройствах, а также скорее всего не смогут загрузить стандартное изображение на BYOD с антивирусом или другими защитным программами. Для этой и

других проблем нам еще придется искать новые инновационные решения. Невзирая на риски, мобильные телефоны, оборудованные элементом безопасности или эквивалентным защищенным контейнером, предоставляют возможности для использования мощных новых моделей аутентификации, с применением телефона в качестве надежного портативного носителя идентификационной информации. Это позволяет использовать его в самых различных ситуациях: от сильной аутентификации прикосновением для удаленного доступа к данным до входа в здание или квартиру.

Мобильность оказывает постоянное влияние на конвергенцию, побуждая команды по физической и ИТ-безопасности сотрудничать при разработке нового решения. Результатом может стать решение простого и эффективного управления PACS-картами и картами IT-доступа на телефонах при обеспечении прежнего уровня безопасности, свойственного картам.

Осознавая преимущества истинной конвергенции

Способность комбинировать управление доступом к физическим и ИТ-ресурсам на одном устройстве, которое может использоваться в самых различных ситуациях, повышает удобство использования, одновременно повышая уровень безопасности и снижая расходы на внедрения и эксплуатацию. Подобное решение устранит необходимость разделять процессы предоставления и регистрации ИТ и PACS-профилей. Более того, теперь с целью конвергенции всей организации к единому комплекту управляемых профилей можно применять унифицированный набор процессов. Организации получат возможность без проблем обеспечивать доступ к зданиям и таким ИТ-ресурсам, как компьютеры, сети, данные и облачные приложения. Эффективное решение при необходимости также может обеспечить безопасность доступа к другим ресурсам, что позволит поддерживать абсолютно операционно-совместимую многоуровневую стратегию безопасности, способную защитить здания, сети, системы и приложения организации сегодня и в будущем.

© 2014 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design, iCLASS, iCLASS Seos, MIFARE and MIFARE DESFire are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

2014-06-05-hid-converged-access-wp-ru PLT-02011