ФИРМЕННОЕ ОПИСАНИЕ

Объединение бизнес-систем: 5 важных шагов, с которых стоит начать

ОБЪЕДИНЕНИЕ СИСТЕМ КОНТРОЛЯ ДОСТУПА, ТЕХНОЛОГИЙ ЗАЩИЩЕННОЙ ПЕЧАТИ И ДРУГИХ ВАЖНЫХ СИСТЕМ ДЛЯ ПОВЫШЕНИЯ УДОБСТВА В РАБОТЕ И УРОВНЯ БЕЗОПАСНОСТИ

Умное рабочее место
Умное рабочее место позволяет однократно выполнить проверку личности пользователя и после проверки предоставлять доступ к различным системам, обеспечивая передачу данных о доверенном идентификаторе во все необходимые системы. Этот принцип кросс-платформенной идентификации делает доступ удобнее и безопаснее.

Доверенный идентификатор
Проверенный с использованием биометрических технологий идентификатор на карте, мобильном устройстве или носимой электронике

Раньше использование смарт-карт для входа в здание было революционной технологией. Сегодня средства идентификации усовершенствованы настолько, что сотрудники могут использовать пропуск не только для входа в здания, но и с его помощью регистрировать время прибытия, пользоваться технологиями защищенной печати и многими другими возможностями — создавая экосистему, которую мы называем рабочим пространством.

Для организаций это означает повышение удобства работы и уровня безопасности за счет объединения разрозненных систем и средств идентификации в единую инфраструктуру. Сотрудники таких организаций могут тратить меньше времени на перемещение, использовать гибкие рабочие станции и рассчитываться в кафетериях и торговых автоматах с помощью технологий безналичного расчета. Развитие оптимизированных рабочих пространств привело к тому, что многие производители столкнулись с повышением спроса на системы с контролем идентификационных данных. С чего же начать?

В данном информационном документе приведено описание первых самых важных пяти шагов при внедрении систем контроля личности. Благодаря этим указаниям производители оборудования смогут предложить клиентам товары и услуги высшего качества. Здесь перечислены вопросы, которые стоит задать, и полезные рекомендации по установке устройств контроля идентификационных данных и их интеграции в бизнес-системы.

За последние годы количество систем с контролем личности существенно возросло. Существует несколько способов расширить диапазон функций систем идентификации личности с использованием карт.

Учет рабочего времени
Быстрый и надежный контроль посещений, при котором невозможно отметиться за отсутствующего коллегу

Защищенная печать
Безопасная технология печати документов, позволяющая снизить затраты и повысить уровень безопасности конфиденциальных данных

Лифт/турникет
Доступ в охраняемые зоны без задержек

Управление автостоянкой
Управление доступом на стоянку для гостей и посетителей

Аутентификация пользователей в сети
Вход и выход в систему через универсальные рабочие станции упрощают совместную работу и повышают уровень безопасности

Управление конференц-залами
Предоставляйте или отзывайте права доступа в конференц-залы для посетителей и сотрудников

Шаг первый: оценка существующих организационных требований и инфраструктуры
Самый главный шаг — тщательное изучение фактических возможностей организации. Идеальное решение должно работать в существующей системе без ее значительных изменений и усложнений. Лучше всего, если технологии контроля личности закладываются в инфраструктуру организации с самого начала. Оценивая состояние и возможности существующей инфраструктуры, необходимо учитывать ряд факторов.

Возможности существующей системы контроля личности. Каким образом происходит использование доверенных идентификаторов и управление ими? Считыватели обращаются к базе данных при каждом использовании, но организации применяют различные процедуры обращения приложений к базам данных. Чтобы определить, будет ли ваша бизнес-система работать с единой центральной базой данных, или необходимо создавать новую, может потребоваться консультация специалиста службы безопасности заказчика. Также можно воспользоваться технологией самостоятельной регистрации, дав возможность пользователям постепенно составить базу данных без вмешательства администраторов. Технологии идентификации личности, например Seos® компании HID, позволяют управлять доступом к различным приложениям и системам при помощи одной карты.

Доступное пространство для размещения новых считывателей. Достаточно ли места? Для идентификации личности с помощью карт и биометрических данных необходима установка считывателей. Оцените доступное физическое пространство для установки считывателей, способ монтажа, а также возможность установки их внутри или снаружи устройства. Внутри корпуса принтера может быть достаточно свободного пространства для установки считывателя или блока обработки, а может потребоваться подключить его вне корпуса в виде отдельного устройства.

Варианты подключения. Как считыватель будет обмениваться данными с базой? Каждый считыватель проверяет данные карты, затем извлекает контрольные данные из базы и передает на соответствующее устройство. Каким образом данные будут передаваться между устройствами, и какой уровень безопасности должен при этом обеспечиваться? Какой тип оборудования, ПО и какие протоколы передачи при этом следует использовать? Чаще всего применяют USB, UART (универсальный протокол асинхронной передачи «приемник — передатчик») и Wiegand для подключения, а также протоколы CCID (аппаратный интерфейс для карт с микрочипом) и KBW (Keyboard Wedge) для передачи данных.

Материалы, используемые в корпусе оборудования. Сколько пространства можно использовать внутри корпуса устройства или рядом с ним? Технология смарт-карт предназначена для работы через воздушную прослойку, любой корпус может ослабить сигнал вплоть до полной его блокировки. Если считыватели устанавливаются внутри корпуса, учтите, что пластиковый корпус пропускает сигнал намного лучше металлического. Установка в изначально не предназначенное для этого оборудование возможна, но может снизить рабочие характеристики системы. Работоспособность биометрических систем в меньшей степени зависит от материала корпуса.

Шаг второй: определение характера взаимодействия с пользователем
Для организаций важны безопасность *и* удобство в работе. Чтобы предложить заказчику оптимальное решение, необходимо точно определить фактические потребности работодателей и сотрудников. Рассмотрим самые важные факторы.

Скорость. Как быстро считыватель устанавливает личность человека? Это зависит от условий эксплуатации. В зонах повышенной безопасности может потребоваться многоуровневая проверка, например, может быть необходимо полностью вставить карту в приемник, а также считать отпечаток пальца биометрическим сканером. В случае, когда требуется меньший уровень безопасности, но намного большая пропускная способность, например в вестибюле учреждения, где сотрудники должны быстро проходить через турникеты, использование мобильных устройств на короткой дистанции или касание носимой электроникой позволяет быстро идентифицировать предъявителя.

Диапазон считывания. Как близко должна находиться карта от считывателя в конкретных условиях? Считыватели могут реагировать на карты или устройства на различных дистанциях в зависимости от требуемого уровня безопасности. Так некоторые считыватели могут распознавать сотрудника, который носит

средство идентификации на себе, при этом предъявлять, например, пропуск необязательно. На объектах со строгой системой безопасности может потребоваться вставить карту в приемник для считывания и передачи многоуровневых данных. Следует отметить, что понятие «дистанция считывания» больше относится к сфере ощущений, чем к точным значениям. Сотрудник может считать, что система разрешила доступ, как только он приложил телефон к считывателю, но на самом деле считыватель уловил сигнал телефона раньше и начал обрабатывать информацию, когда человек еще не подошел к устройству вплотную.

Опыт администратора ИТ-систем. Обладают ли сотрудники ИТ-службы заказчика достаточным опытом и квалификацией? В мелких компаниях может не хватать сотрудников для создания новых баз данных и управления ими, как и для установки новых блоков обработки. Для крупных компаний может потребоваться настройка конфигурации удаленного обновления, позволяющей обновлять тысячи считывателей без необходимости выезда для этого сотен специалистов на отдельные объекты.

Шаг третий: определение и изучение используемой технологии

Технологии постоянно развиваются, поэтому оценивать следует как возможности используемой технологии в настоящий момент, так и планы заказчика на будущее. Так как цель — максимально использовать возможности существующей системы, в существующей модели необходимо учесть развитие в будущем. Следует учесть фактор мобильных систем аутентификации, так как даже если компания в настоящее время не использует мобильные средства аутентификации, она, вероятно, начнет их использовать в будущем. Большинство организаций используют комбинацию описанных ниже технологий.

Мобильный доступ
Технологии мобильного доступа делают смартфон или смарт-часы сотрудника пропуском. Контроль доступа на объекты и в системы организации с использованием идентификаторов на мобильных устройствах обеспечивает высокий уровень безопасности и удобства.

RFID. Радиочастотная идентификация часто используется в картах и носимой электронике, это самая распространенная технология безопасности.

NFC. Стандарт ближней радиосвязи NFC используется для контроля доступа с помощью карт, мобильных устройств и носимой электроники.

BLE. Bluetooth Low Energy чаще всего используется для поиска и контроля состояния с помощью мобильных устройств и носимой электроники.

Биометрия. Несмотря на сложность реализации, этот вариант обеспечивает самый высокий уровень безопасности, а зачастую он удобнее остальных, так как не требует носить с собой дополнительные средства идентификации.

Шаг четвертый: выбор самого подходящего форм-фактора считывателя

Системы идентификации имеют разные уровни сложности, а организации могут иметь разные возможности. Чтобы определить вариант реализации, максимально подходящий организации, технические возможности лучше всего обсуждать с инженером или приглашенным сторонним специалистом. Существует несколько исполнений считывателей.

Блок обработки считывателя. Блок обработки или процессор Secure Element (SE) — обязательный элемент, уникальный для каждой модели считывателя. Организации, в штате которых есть квалифицированные технические специалисты, разрабатывают печатные платы с блоком обработки специально для бизнес-систем. Устройство биометрической аутентификации в исполнении блока обработки не выпускается.

Ядро считывателя. Комбинация микрочипа и элементов ядра (без антенн) позволяет считывателю передавать данные через протоколы RFID, BLE и пр., но не поддерживает биометрию. Ядро считывателя обычно выбирают производители, если хотят разработать антенну собственной конструкции, которая должна поместиться в существующее пространство.

Модуль считывателя. В модуль считывателя входит блок обработки и антенны, но он должен располагаться внутри корпуса существующей бизнес-системы. Модули, считывающие данные карт и биометрические данные, можно встраивать в существующие системы, чтобы обеспечить контроль их использования на основе идентификаторов.

Настольный считыватель. Это отдельный блок, обычно размещаемый на рабочем столе или монтируемый на существующее устройство. Настольные считыватели, например HID Global Omnikey®, — это практически готовое комплексное решение, которое требует только базовых технических знаний, но они занимают намного больше места.

Шаг пятый: разработка считывателя и его интеграция в существующие устройства

Самый важный фактор при выборе и интеграции считывателя — поддерживает ли соответствующие функции существующий принтер, лифт или система контроля рабочего времени. Новая система контроля идентификационных данных должна быть удобнее, а не сложнее предшествующей. Рассмотрим несколько аспектов, которые важно учесть.

Связь с сервером. База данных, считыватель и карта доступа должны обмениваться информацией в понятном им всем формате.

Эстетика. В идеальном варианте считыватель должен быть составляющей частью существующего устройства, а не криво прикручен сбоку.

Тестирование и техническая поддержка. С тестовыми картами поставляется инструментарий разработчика для различных систем, позволяющий администраторам проверять качество пользовательского взаимодействия перед реализацией. HID Global также предлагает профессиональные услуги для производителей оригинального оборудования, интеграторов и клиентов. Данные услуги входят в портфель Extended Access Technologies (EAT).

Заключение

Расширяйте существующую инфраструктуру с учетом будущих требований

Возможность использовать одно и то же средство идентификации для доступа к различным системам значительно упрощает работу. При этом снижаются затраты, и повышается темп работы в долгосрочной перспективе, а также снижается вероятность человеческих ошибок. Самое главное — интеграция разрозненных систем необязательно сопровождается полным изменением инфраструктуры. Оптимизированное рабочее пространство можно создать с учетом конкретных требований на основе существующих систем и с оплатой по факту выполнения.

HID Global предлагает широкий ассортимент считывателей и карт для любых сфер деятельности, а также услуги технической поддержки и обслуживание на всех этапах. Более подробная информация о наших системах контроля идентификационных данных приведена в информационном бюллетене «*Оптимизированное рабочее пространство*» по прямой ссылке или на нашем веб-сайте.

2019-03-16-hid-eat-make-bus-syst-id-aware-wp-ru

PLT-04751