ФИРМЕННОЕ ОПИСАНИЕ

Внедрение технологии защищенной печати

Что такое доверенный идентификатор?

Доверенный идентификатор — это проверенный при использовании биометрических или других технологий идентификатор на карте, мобильном устройстве или носимой электронике. В умном офисе такой идентификатор можно использовать для доступа к различным системам, например для доступа в здания, контроля времени и длительности посещений, а также защищенной печати.

Как использовать существующие идентификаторы для простой и безопасной печати?

Безопасная и простая печать

После печати конфиденциальный документ может легко попасть в руки злоумышленников. Это очень серьезная и часто игнорируемая угроза безопасности. Около 70% организаций подвержены рискам, связанным с печатью документов. Многие испытывают сложности в связи с отслеживанием назначений и ошибок при невозможности точно идентифицировать пользователя. Кроме того, наиболее распространенные методы «защищенной» печати или слишком сложны в освоении, или слишком ненадежны в плане защиты. Например:

- панели для ввода PIN-кода — это удобное устройство, ведь не нужно носить с собой средства идентификации, но для его использования необходимо, чтобы пользователь точного помнил код и никому его не сообщал;
- пароли часто теряют, забывают или передают третьим лицам, из-за чего ИТ-службам организаций приходится постоянно обновлять, изменять или отзывать пароли;
- QR-коды очень просто копировать и клонировать, из-за этого создается ложное ощущение безопасности.

Эффективный способ решения перечисленных задач — реализовать встроенную в программы печати технологию контроля идентификационных данных. Функция защищенной печати в сочетании с существующей системой доверенных идентификаторов — бейджей, мобильных устройств и биометрических технологий — повышает уровень безопасности и удобства для пользователей, а также проста в реализации для производителей принтеров и их партнеров. Этот документ предоставляет организациям информацию о технологиях защищенной печати и двух ее основных составляющих: средствах идентификации и считывателях для них. После его прочтения вы будете знать основы технологии защищенной печати и о том, как ее можно использовать в существующей системе управления безопасной идентификации.

Безопасность, экологичность и экономичность: технология защищенной печати

Без функции защищенной печати документы отправляются на печать и сразу же выходят из принтера. Этот принцип обеспечивает безопасность только при условии, что пользователь сразу может забрать бумажный экземпляр в момент выхода из принтера (например, если принтер находится непосредственно возле рабочего стола сотрудника). В связи с тем, что нецелесообразно предоставлять каждому пользователю персональный принтер, большинство заданий печати выполняется централизованно на некотором удалении от рабочих мест сотрудников.

Эта ситуация часто наблюдается в учреждениях здравоохранения, где врачи проводят осмотр пациентов в кабинетах, вводят данные в систему с помощью ноутбука и делают бумажные копии документов на центральном принтере административного здания. Конфиденциальная информация пациентов остается в приемном лотке принтера, пока ее не заберут сотрудники или кто-либо, находящийся возле принтера.

Конфиденциальность — не единственный фактор, на который следует обратить внимание. Сертификация оборудования в сфере защиты окружающей среды и репутация экологически безопасной продукции все больше привлекает покупателей.

При использовании функции защищенной печати документы не будут отправлены на печать сразу. Вместо этого операция печати может находиться в состоянии ожидания, пока врач или уполномоченное лицо не подтвердит личность с помощью той же карты, мобильного устройства или биометрических данных, которые используются для других целей (например для доступа в здание или на служебную стоянку). Врач, пациент и аудиторы HIPPA могут быть уверены, что доступ к информации может получить только лицо, имеющее на это право. Эта технология позволит компаниям в любой отрасли экономики достичь достаточно высокого уровня конфиденциальности, особенно с учетом новых более строгих правил, в частности, GDPR, и растущей ориентированности на замкнутость бизнес-систем.

Конечно, конфиденциальность — не единственный фактор, на который мы обращаем внимание. Сертификация оборудования в сфере защиты окружающей среды и репутация экологически безопасной продукции все больше привлекает покупателей. Компании, взявшие на вооружение принцип триединства, стараются внедрять экологически безопасные инициативы, но и те предприятия, которые не принимают участия в мероприятиях такого рода, стремятся сократить лишние расходы. В этом поможет технология защищенной печати. Приблизительно 20% бумажных копий документов получает не тот пользователь, который инициировал печать, что ежедневно приводит не только к дополнительным затратам и увеличению количества отходов, но и к возрастанию нагрузки на бюджет отделов. Если используется функция защищенной печати, документы остаются в очереди на сервере до получения разрешения на печать, благодаря чему снижаются затраты и негативное влияние на экосистему планеты.

Но не все методы защищенной печати одинаково эффективны. Создание правильной программы требует знания конфигурации вашей системы и требований, а также сотрудничества на начальном этапе реализации проекта. В конце концов, полностью заменять существующую систему новой — это нецелесообразно ни с экологической, ни с экономической точки зрения. Для получения эффективного результата необходимо

изучить существующую систему

Задайте вопрос: какой механизм аутентификации будет использовать ваша организация для защищенной печати? Большинство предпочитает работать с уже существующими удостоверениями и пропусками, то есть дооснащать существующие системы новыми функциями, а не создавать систему с нуля. Конечно, это неприменимо в случае, когда существующая система устарела, и ее необходимо полностью менять. Подумайте, как пользователи будут работать с функцией защищенной печати в ближайшем и отдаленном будущем.

Если вы используете карты/бейджи:

карты — одна из самых распространенных технологий, используемых с функцией защищенной печати. Сегодня существует несколько технологий аутентификации, и в будущем значение карт снизится, но их все равно будут использовать еще долго. Тип карт, их торговая марка и ваши требования определяют тип считывателей, которые должен будет поставить производитель принтеров, и уровень защиты, который они обеспечивают. Ниже перечислены самые распространенные виды карт.

Бесконтактные карты. Карты с частотой 125 кГц очень просты в использовании: необходимо лишь поднести карту к принтеру, и задание печати будет выполнено. К сожалению, они обеспечивают самый низкий уровень безопасности. Бесконтактные карты назначают человеку серийный номер, который передается на считыватель, но такой номер относительно легко клонировать.

Смарт-карты. Смарт-карты, например HID Seos®, используют случайно сгенерированные серийные номера для установления связи со считывателем, что практически устраняет возможность клонирования. Также эта технология позволяет избежать коллизии: когда две бесконтактные карты находятся одновременно возле считывателя, считыватель может не работать корректно, а в случае со смарт-картами считыватель выбирает правильную карту.

Технологии доступа с помощью мобильных устройств и носимой электроники не должны быть привязаны к определенному бренду.

Метки/наклейки. Если вы используете устаревшую технологию карт, или ваши карты не поддерживаются производителем принтеров, для упрощения связи со считывателем можно использовать метку или наклейку. Метки работают на той же частоте, что и бесконтактные карты (125 кГц), и не обеспечивают такой уровень безопасности, как смарт-карты.

Несколько типов карт. В крупных организациях можно одновременно использовать несколько типов карт в зависимости от расположения объекта и уровня безопасности. Например, в головном офисе компании для доступа в здание можно использовать технологию Seos®, а в филиалах — бесконтактные карты. Некоторые считыватели могут считывать карты различных типов — поставщик или производитель должен знать о таком требовании.

Если вы используете или планируете использовать для аутентификации мобильные устройства или носимую электронику.

Доступ с помощью мобильных устройств переживает рост популярности. Если в настоящий момент вы не используете эту технологию, вполне возможно, что вы обратитесь к ней в будущем. Если вы используете карты, можно дополнительно заложить в считыватели функцию считывания информации с мобильных устройств. Это позволит перейти на использование мобильных идентификаторов с минимальными изменениями.

Мобильные устройства и носимая электроника, как и все альтернативные технологии, имеют несколько уровней безопасности. QR-коды на экране мобильного телефона относятся к относительно небезопасным вариантам, так как их довольно легко скопировать. Bluetooth-маячки и метки NFC, с другой стороны, обеспечивают более высокий уровень защиты и не допускают копирования. Мобильные идентификаторы удобнее в развертывании и управлении, чем карты, так как обновления можно рассылать мгновенно без необходимости выезжать на объект.

Технологии доступа с помощью мобильных устройств и носимой электроники не должны быть привязаны к продуктам определенного бренда. Например, ваша система защиты печати с помощью мобильных идентификаторов должна работать для пользователей как iPhone, так и Android.

При использовании биометрических технологий:

биометрия, например считывание отпечатков пальцев, обеспечивает достаточно высокий уровень безопасности и удобства использования. Учитывая более высокий уровень безопасности, неудивительно, что стоимость таких средств существенно выше. Многие организации предпочитают биометрию прочим технологиям, в том числе картам и мобильным идентификаторам. Биометрические решения имеют несколько уровней безопасности. Государственные органы и другие организации, где необходим высокий уровень безопасности, в дополнение к сканированию отпечатков пальцев используют технологии распознавания искусственных отпечатков и дыхания.

Сформулируйте требования к считывателю

После того как вы нашли производителя, продукция которого соответствует возможностям ваших систем и средств идентификации, нужно выбрать тип считывателя, используемого для защищенной печати. Сначала необходимо установить, на каком расстоянии считыватель должен определять присутствие идентификатора: нужно ли пользователю подходить вплотную к принтеру для запуска печати? Карты, биометрия и некоторые технологии с использованием мобильных устройств и носимой электроники требуют, чтобы пользователь коснулся считывателя или приложил к нему карту или устройство, и смог тут же забрать отпечатанные листы. С другой стороны, для упрощения процедуры и ускорения работы может быть допустимо, чтобы принтер улавливал сигнал от средства идентификации с расстояния в пару метров.

Правильно подобранное решение сочетает безопасность и удобство, приближая вас еще на один шаг к оптимизации рабочего пространства.

Потом нужно определить, должен ли считыватель находиться внутри принтера, или его можно установить снаружи. Встроенные считыватели обеспечивают более эстетичный внешний вид оборудования, но требуют наличия свободного пространства внутри корпуса принтера и возможности доступа для установки и проведения технического обслуживания. Считыватели в отдельном корпусе или в настольной конфигурации, с другой стороны, похожи на небольшой жесткий диск, который подключен к принтеру кабелем и может быть при необходимости заменен. Считыватель в настольной версии также не подвержен воздействию помех от корпуса принтера.

Считыватели могут отличаться по совместимости. Даже если в организации используются исключительно карты Seos®, считыватель может не принимать карты с одного объекта при попытке использования на другом. Кроме того, не все считыватели могут работать с любыми идентификаторами. Например, если вы используете карты, но планируете переходить на мобильные идентификаторы, нужно выбирать считыватель, который может работать с обеими технологиями.

После необходимо выбрать доступные виды связи и технологии передачи данных. Например:

- ¡ USB-разъемы позволяют подключать внешние устройства, автоматически настраивать антенну считывателя и выполнять регулировку параметров на месте. Для биометрических считывателей подключение по USB — самый удобный способ подключения и настройки.
- ¡ UART-подключение требует установки считывателя внутри корпуса принтера и отличается сложностью в настройке.

Проконсультируйтесь со своим главным союзником — производителем принтеров или поставщиком услуг печати.

Несмотря на то, что технически вы можете купить считыватели самостоятельно и поставить перед ИТ-специалистами задачу подключить их, мы не рекомендуем этот способ: он может привести к излишней трате времени и ресурсов. Обсуждение ваших существующих требований и планов, соответствующей дистанции считывания и подтверждения присутствия, а также расположение считывателей относительно принтера с поставщиком или производителем обеспечит качественную и беспроблемную реализацию проекта внедрения.

Найдите собственное решение

Изучение основ технологии защищенной печати, а также своих существующих и будущих требований помогут направить переговоры с поставщиком или производителем в нужное русло. Они имеют наибольшее влияние на процесс внедрения технологии защищенной печати, так как могут предложить именно тот вариант, который максимально подойдет вашей организации, и порекомендовать отказаться от ненужных функций. Правильно подобранное решение сочетает безопасность и удобство, приближая вас еще на один шаг к оптимизации рабочего пространства. Организации экономят значительные средства за счет использования общих принтеров, отказа от бумажного документооборота, снижения количества отходов и более эффективного распределения затрат.

Лучший способ — использовать уже знакомые пользователям и ИТ-специалистам средства идентификации, так как это потребует меньших затрат на обучение. Ваше новое решение станет дополнением к существующей системе идентификации и новым шагом к по-настоящему оптимизированному рабочему пространству.

На нашем веб-сайте вы сможете узнать больше об ассортименте считывателей для защищенной печати.

[1] Исследование Quocirca: http://quocirca.com/wp-content/uploads/2018/06/Quocirca-Print-Security-Jan-2017-Report-Excerpt.pdf

[2] Исследование Nuance: https://whatsnext.nuance.com/office-productivity/orphaned-print-jobs-silent-security-leak/

2019-05-06-hid-eat-secure-print-wp-ru

PLT-04762