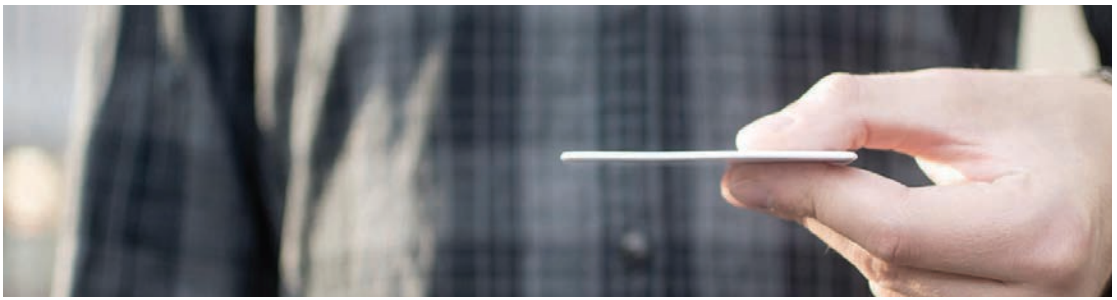


zwipe™

A world without PINs and passwords

Карты доступа Zwipe Access со сканером отпечатка пальца

ЗНАКОМСТВО С БИОМЕТРИЧЕСКИМИ КАРТАМИ

STA GROUP

Группа компаний «СТА» – эксклюзивный представитель Zwipe в Украине, странах СНГ и Прибалтике

Понятие идентификации, как процедуры установления тождества личности с заранее предустановленным шаблоном, – одно из ключевых для систем контроля и управления доступом. Регламентировать доступ к определенным закрытым зонам или объектам представляется возможным
только в том случае, когда СКУД четко различает пользователей по параметру «свой-чужой».

Предлагаем вашему вниманию уникальный продукт – бесконтактные прокси-карты со встроенным сканером отпечатка пальца.

Владельцу карты необходимо приложить палец к сканеру на карте, и только в случае совпадения отпечатка с записанным в памяти образцом карта передает сигнал на считыватель.

zwipe™

A world without PINs and passwords

ZWIPE
ЗНАКОМСТВО С БИОМЕТРИЧЕСКИМИ КАРТАМИ

КАРТЫ ДОСТУПА

На протяжении вот уже нескольких десятков лет основным средством идентификации в СКУД являются различного рода карточные продукты. Это могут быть контактные и бесконтактные карты различных форматов и стандартов, QR (двухмерные)- и штрих-коды на различных физических и электронных носителях и даже смартфоны со встроенным чипом NFC. Широкое распространение подобного рода идентификаторов объясняется прежде всего их низкой стоимостью, а также универсальностью – карты доступа легко добавлять в любую уже существующую СКУД. Кроме того, т.н. смарт-карты (группа продуктов под общим брендом Mifare), благодаря наличию встроенной памяти, могут быть использованы для различных сторонних приложений: муниципальные транспортные системы, программы лояльности и пр.

Однако карты доступа имеют ряд существенных недостатков, которые, если задуматься, сводят к нулю попытки организации строго контроля и учета потоков посетителей и сотрудников.

Карта – это предмет, а не человек

И любая, даже самая функциональная СКУД, будет идентифицировать именно кусок пластика, а не индивидуума, который его предъявляет. Таким образом, системы, построенные с использованием карточных продуктов, выполняют функцию идентификации очень условно: контролирующий орган игнорирует факт возможности подмены фактического пользователя карты неавторизованным, а пользователь делает вид, что он не пользуется этой возможностью.

Реальность же часто совсем иная. В зависимости от воли пользователя, проблему необходимо рассматривать в двух плоскостях. Во-первых, он может целенаправленно передать свой идентификатор сторонним лицам для выполнения противоправных действий. Как часто, например, контролер сталкивается с фактами, когда пользователь физически отсутствовал на рабочем месте, но согласно отчетам СКУД – время отработано и за него необходимо заплатить. Выявить такие факты сложно, еще сложнее бороться с ними.

Во-вторых, пользователь, сам того не желая, может банально потерять карту. И если, нашедший ее злоумышленник, по стечению обстоятельств знает куда и когда она предоставляет доступ, суммы потенциального ущерба от неавторизованного проникновения могут быть весьма значительны.

ЗАЩИТА ДАННЫХ ОТ ПЕРЕЗАПИСИ

Второй серьезной проблемой карточных идентификаторов является техническая возможность их клонирования. Немногие знают, но самый распространенный в нашей стране стандарт бесконтактных карт EM-marine (от 70% до 80% всех СКУД используют именно его для идентификации) вообще не имеет защиты от несанкционированного считывания и последующего клонирования.

Почти все карты доступа могут быть клонированы

Теоретически несколько лучше обстоят дела с картами семейства Mifare на базе чипов производства NXP Semiconductor. Для защиты данных в них используются лицензионные проприетарные криптоалгоритмы и идентификаторы Mifare Plus/Mifare Desfire EV-1 действительно оснащены серьезной защитой. Но как всегда, есть маленькая оговорка: число проектов реализованных с использованием карт этих двух стандартов активно стремится к нулю. Это связано в первую очередь с их стоимостью. Кроме того, предложение совместимых считывателей и база опыта и знаний относительно их правильного применения также кажутся недостаточными.

Стандарт Mifare Classic более популярен, в том числе благодаря и возможности производить карты на базе неоригинального тайваньского чипа, совместимого с протоколами NXP. Стоимость таких продуктов близка к EM-Marine. Однако, защита этих карт была взломана еще в 2008 году.

Таким образом, имея определенные технические средства, злоумышленник сможет на небольшом расстоянии считать данные карты и восстановить их на другой карте.

БИОМЕТРИЧЕСКИЕ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА

Теоретически все недостатки СКУД на базе карточных идентификаторов могут быть устранены биометрическими терминалами. Вопреки расхожему мнению, разработка методов, принципов, а позже и систем распознавания биометрических характеристик человека имеет длинную и интересную историю, насчитывающую уже почти сто лет.

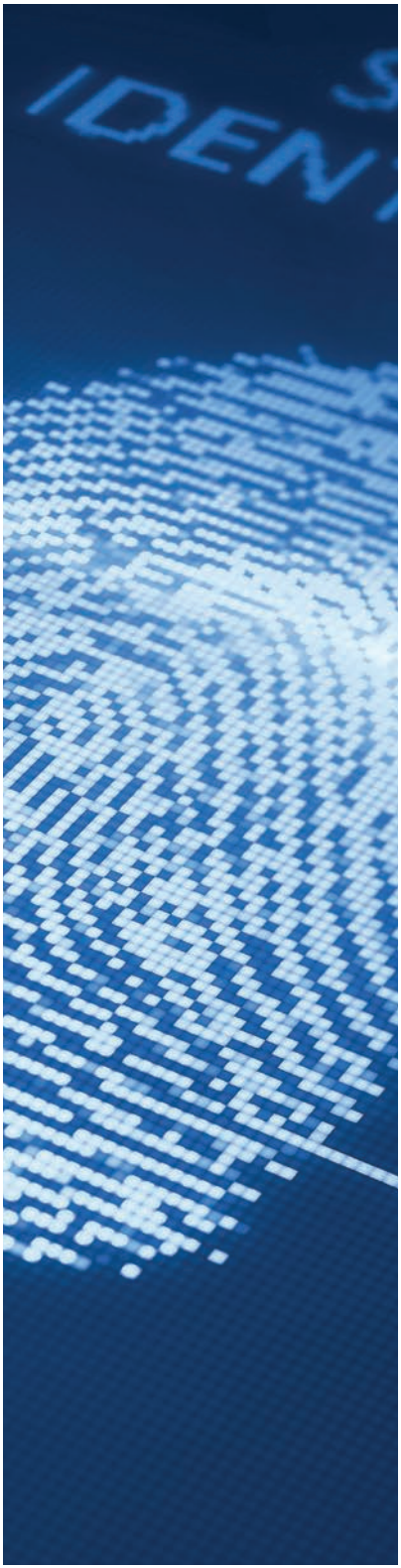
Однако в повседневной жизни биометрические СКУД до сих пор встречаются редко. Действительно существует много офисов, бизнес-центров, даже крупных промышленных предприятий, где биометрия положена в основу системы учета сотрудников и посетителей организаций, но их удельный вес в общей массе установленных и эксплуатируемых систем контроля доступа остается незначительным.

Конечно, пользователь не имеет возможности сознательно передать свой биометрический идентификатор третьему лицу или потерять его. Дублировать и воспроизвести биометрический параметр на другом носителе – также задача не из легких (хотя в зависимости от типа параметра, в принципе возможная).

Но сам современный принцип работы биометрических терминалов создает ряд сложностей, препятствующих их повсеместному распространению. Во-первых, это конечно же цена.

Высокая стоимость дактилоскапических терминалов существенно препятствует широкому распространению биометрических систем контроля доступа

Стоимость контактных дактилоскопических терминалов даже азиатского производства, как самого популярного и доступного биометрического решения, в разы, а то и десятки раз превышает стоимость считывателей карт доступа. Устройства, в основе которых, лежит распознавание других параметров (геометрия руки, лица, венозного рисунка, радужной оболочки глаза и др.) будут еще дороже. Уже на этом этапе большинство потенциальных заказчиков СКУД предпочитают работать с простыми и понятными инструментами карточного доступа, несмотря на все их недостатки.



СОВМЕСТИМОСТЬ ОБОРУДОВАНИЯ И СИСТЕМ

Вторым очень важным моментом является, безусловно, совместимость. Автору не приходилось встречать рекламных буклетов или других материалов производителей биометрических терминалов, которые бы не содержали фразы типа «простая интеграция с любыми системами СКУД». Это не совсем так и здесь необходимы некоторые пояснения.

Идентификация объекта и принятие решения

В стандартных системах на базе карт сопоставлением образца (т.е. предъявленного идентификатора) и шаблона или образа (в данном случае номера конкретного идентификатора, заранее записанного в базу) занимается контроллер. Считыватель лишь транслирует полученный номер карты для обработки. В подавляющем большинстве биометрических систем мэтчинг (именно так правильно называется этот процесс) выполняется самим считывателем или терминалом.

После успешной процедуры мэтчинга возможен один из двух вариантов.

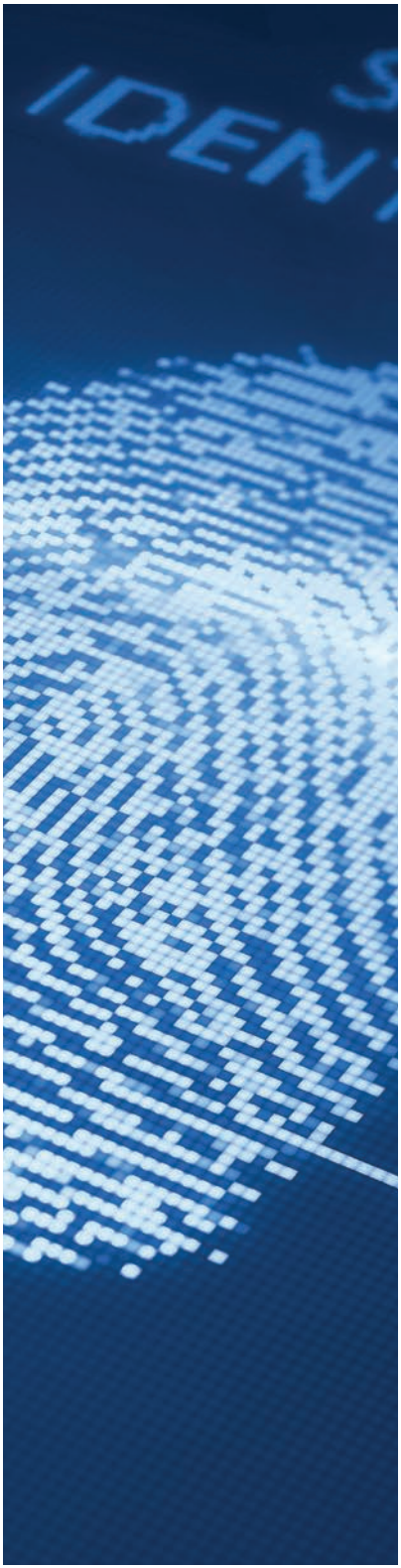
1. Терминал сам принимает решение и таким образом выполняет функцию контроллера (управление замком может происходить через встроенное реле)
2. Терминал формирует пакет данных и отправляет его на сторонний контроллер СКУД для обработки.

Первый вариант выглядит изначально очень привлекательным: большинство терминалов имеют возможность сетевого подключения по TCP/IP и реле управления замками. Все, что необходимо для получения законченной СКУД – это программное обеспечение для добавления/удаления пользователей и настройки правил и алгоритмов доступа.

Почти все производители биометрических терминалов предлагают собственное ПО

Однако, тут и возникает проблема. В подавляющем большинстве случаев оно обладает весьма скромным функционалом и годится исключительно для внесения новых пользователей в БД или для организации доступа в небольшом офисе. Серьезную систему учета на его базе построить невозможно, не говоря уже об интеграции в нее сторонних комплексов, например видеонаблюдения или охранной сигнализации.

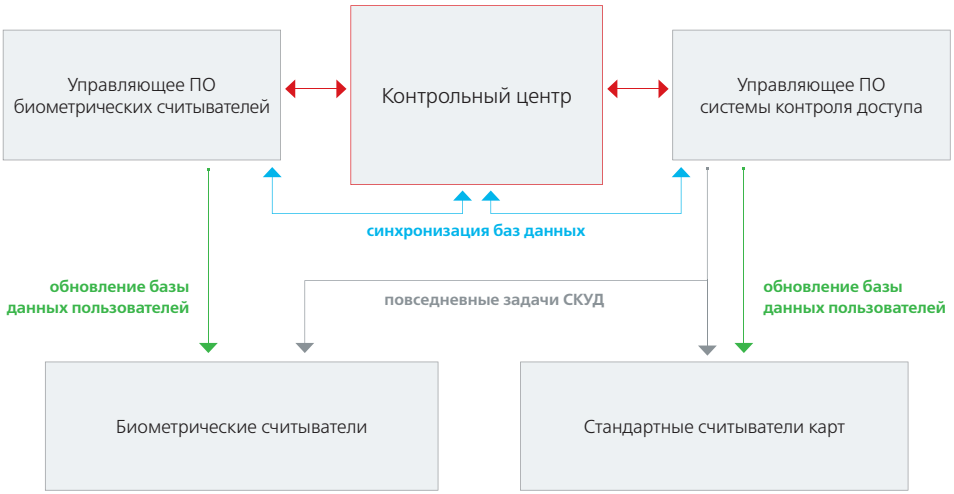
Зачастую удел подобных решений – примитивные задачи с ограниченным количеством пользователей. Справедливости ради нужно сказать, что процент таких инсталляций все же высок.



Биометрические терминалы в составе крупных систем

Эксплуатация биометрических средств идентификации в составе серьезных систем СКУД однозначно предполагает второй вариант. В этом случае биометрический терминал по сути рассматривается контроллером СКУД как обычный считыватель выдающий информацию об идентификаторе в протоколе Wiegand (благо таким выходом оснащены почти все современные терминалы).

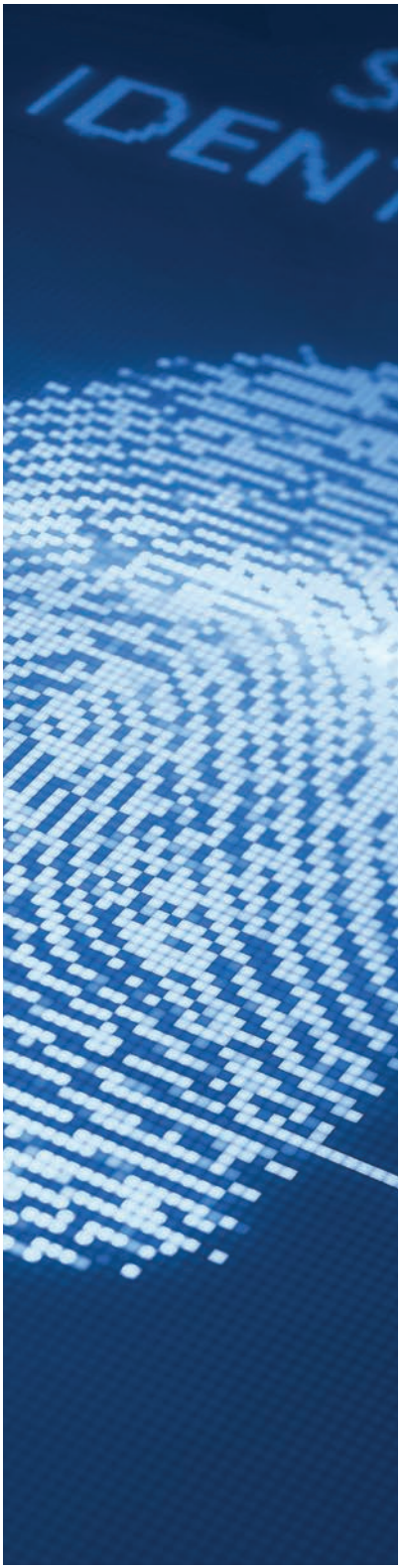
И все было бы просто, если бы не тот самый мэтчинг, все равно производящийся самим считывателем. Другими словами, оператору системы необходимо добавлять/удалять биометрические идентификаторы во все считыватели посредством родного ПО терминалов, а вот выполнять связанные с КД повседневные задачи уже из программы системы контроля и управления доступом.



Наличие у терминалов выхода Wiegand для совместимости на практике дает немного

Можно предположить, что для объектов с минимальной «текучкой кадров» и отсутствием сторонних посетителей этот вариант может быть приемлем. Но следует напомнить, что такая схема применяется при реализации серьезных задач учета, а значит и вероятность постоянного изменения структуры базы данных пользователей достаточно высока. Постоянная же работа с двумя ПО выглядит по меньшей мере неудобно. Кроме того, оператору будет необходимо постоянно синхронизировать базы данных биометрических терминалов и СКУД, и делать это придется скорее всего в ручном режиме (в топовых СКУД предусмотрена возможность автоматической синхронизации, но для этого необходима глубокое сотрудничество между производителями обеих систем).

Так что, наличие у терминалов выхода Wiegand, как основы заявления о полной совместимости, на практике дает немного.



ЗАЩИТА БИОМЕТРИЧЕСКИХ ДАННЫХ

Вопрос безопасности персональных биометрических данных человека также поднимается Заказчиком достаточно часто. Несмотря на то, что проблема эта абсолютно надуманная, потенциальные пользователи подобных систем могут негативно относиться к процедуре сбора отпечатков пальцев или других параметров для идентификации.

Дело в том, что нужно четко разграничивать криминалистическую биометрию и электронные системы доступа, основанные на распознавании биометрических характеристик. В последнем случае система никогда не хранит шаблон (например, дактилоскопический отпечаток) в чистом виде. В процессе добавления пользователя в систему, сканер действительно получает изображение того или иного признака (в зависимости от терминала, это рисунок дуг, завитков и петель на коже пальца, структура сетки вен, геометрия ладони с расставленными пальцами и т.д.).

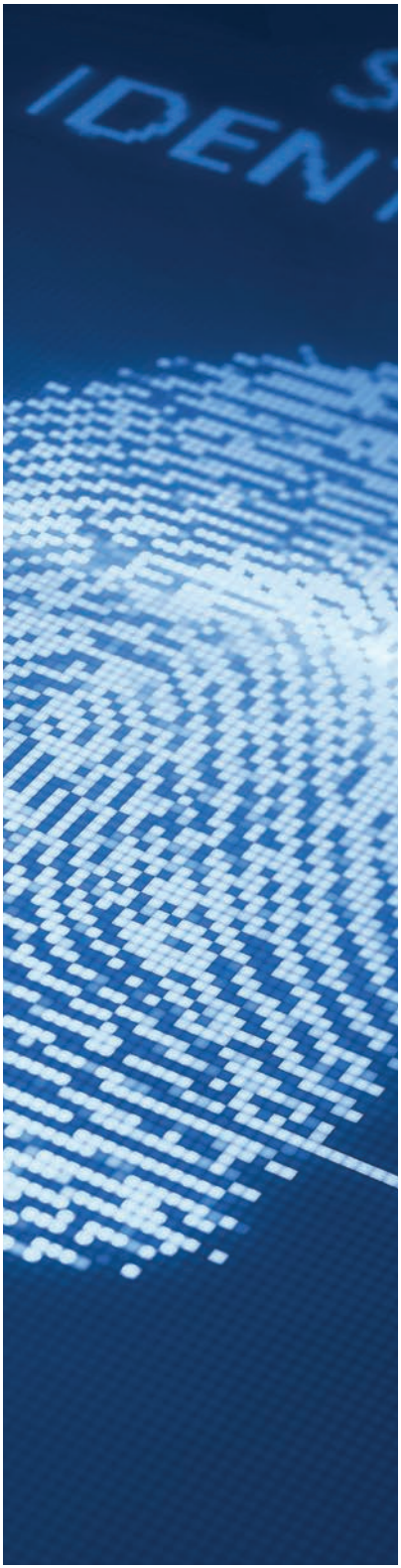
Однако в дальнейшем происходит процесс извлечения из него опорных данных, как расстояние между определенными точками на отпечатке пальца, которые оцифровуются и уже не имеют ничего общего с оригиналом. Какие именно опорные данные будут использоваться для создания виртуального образа идентификатора – информация обычно строго закрытая, и используется каждым конкретным производителем как часть проприетарного алгоритма.

Невозможно восстановить оригинальный рисунок отпечатка из цифрового шаблона

И хотя каждый производитель терминалов уделяет много усилий для объяснения этих тонкостей, часто сознание того, что кто-то может завладеть личными данными, может оттолкнуть Заказчика от выбора в пользу биометрии.

ФИЗИЧЕСКИЙ КОНТАКТ С БИОМЕТРИЧЕСКИМ ТЕРМИНАЛОМ

Последним серьезным недостатком биометрических терминалов является вопрос гигиены.Конечно, существует много техник бесконтактного сканирования биометрических параметров, но все же подавляющее большинство систем реализовано на контактном дактилоскопическом принципе (не в последнюю очередь из-за стоимости, и, наверное, относительной известности данной технологии). А такие терминалы предполагают непосредственный контакт кожи пальца пользователя со сканером.

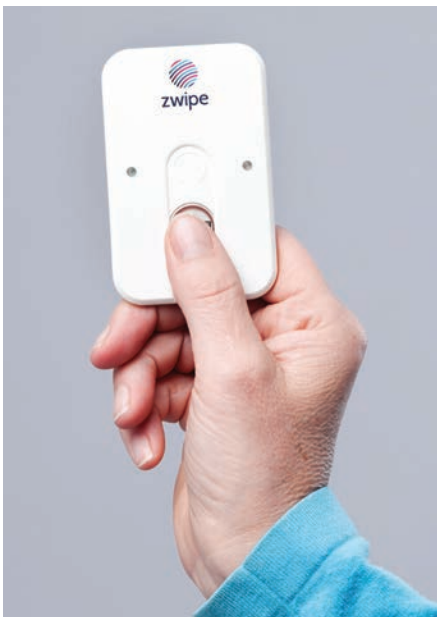


БИОМЕТРИЧЕСКИЕ КАРТЫ ДОСТУПА ZWIPE

Принимая во внимание все вышеизложенные мысли, возникает логичный вопрос: а существуют ли альтернативные идентификаторы, которым не присущи все указанные минусы? Оказывается, да. Еще начиная с 2009 года американский старт-ап Zwipe, финансируемый венчурными инвестиционными фондами из Норвегии, начал разработку принципиально новых устройств идентификации на рынке СКУД.

Идея состояла в объединении всех преимуществ биометрии с простотой и доступностью традиционных карточных продуктов. После нескольких лет активных исследований и разработок компания предложила рынку биометрические карты.

Физически новое устройство размерами и формой действительно напоминает обычную карточку, однако имеет встроенный дактилоскопический сканер



Принцип работы карты Zwipe следующий: пользователь прикладывает заранее внесенный в память палец к сканеру, который активирует соответствующий встроенный в карту транспондер (непосредственно бесконтактную составляющую), и предъявляет последнюю считывателю. Обмен данными между картой и считывателем возможен только тогда, когда отпечаток пальца пользователя совпадает с записанным шаблоном.

Карта, при этом, - одноразовая, т.е. перезаписать отпечаток или каким-либо другим образом модифицировать его невозможно. Таким образом пользователь, а главное владелец СКУД, могут быть абсолютно уверены, что потеря идентификатора не приведет к неавторизованному его использованию сторонними лицами. Передача карты коллеге для противоправной авторизации на объекте также не имеет смысла.

Разработчики Zwipe сумели сохранить все преимущества карточных продуктов, устранив ненадежные с точки зрения СКУД тонкости

Базовой особенностью продуктов Zwipe, кроме того, является и то, что в режиме ожидания (т.е. при отсутствующем на сканере пальце), «завести» транспондер извне для последующего клонирования не представляется возможным: в этом состоянии устройство представляет из себя просто кусок пластика. Поэтому, кстати, тип применяемой бесконтактной технологии становится абсолютно неважным параметром, его выбор регламентируется только уже установленной на объекте инфраструктурой СКУД. Как EM-marine (вообще не содержащий инструментов криптозащиты), так и DESFire EV-1 (самый защищенный на сегодняшний день бесконтактный стандарт) одинаково неуязвимы для устройств негласного съема данных.

ПРЕИМУЩЕСТВА БИОМЕТРИЧЕСКИХ КАРТ

Синергетический эффект объединения двух технологий еще больше проявляется при анализе биометрической составляющей. Так или иначе, а биометрическая карта значительно дешевле даже самого экономичного терминала.

При стоимости менее 100USD, вся математика может принять следующий вид: если принять среднюю по рынку стоимость биометрического считывателя в 500USD, то на объекте с одной дверью и 4 авторизованными пользователями дешевле инвестировать в Zwipe (такой дверью с ограниченным числом лиц, имеющих к ней доступ, может быть, например, вход в хранилище в банке). Далее читатель может произвести расчеты самостоятельно.

Что же касается администрирования биометрических терминалов, одновременного ведения баз данных СКУД и биометрии, работы в нескольких программах, то и здесь продукты Zwipe предлагают пользователю совершенно новый опыт. Мэтчинг происходит непосредственно в самой карте по методу 1:1 (этим, кстати, и обусловлена скорость сопоставления, не превышающая 1,5сек.). А это означает, что нет необходимости в создании дополнительной базы данных, в ее администрировании и защите.

Карты Zwipe могут работать в составе любой, уже установленной системе

Для обеспечения полной, а не заявляемой, совместимости нужно просто выбрать модель с транспондером, аналогичным уже применяемому на объекте. Вся настройка и внедрение, к большому сожалению инсталляторов, ограничивается стандартной процедурой добавления карт в СКУД.

Никаких проблем с защитой персональных данных у владельца системы также не возникнет. Процесс записи пальца выполняется пользователем (а не администратором системы) с помощью самой карты. Даже теоретически дактилоскопические данные не могут быть переданы сторонним лицам. Вопрос гигиены также решается сам собой.

ПЕРСПЕКТИВЫ

Биометрические карты Zwipe – классический пример т.н. «голубого океана», т.е. продукт, создающий не существовавший ранее спрос на новом рынке, где практически отсутствуют конкуренты (см. «Blue Ocean Strategy» за авторством К. Чана и Р. Моборна). Они не призваны полностью вытеснить карточные продукты (учитывая стоимость) или биометрические терминалы.

Карты Zwipe открывают абсолютно новые возможности в сфере СКУД, уводящие интегратора от традиционных малоприбыльных рынков со множеством игроков








Так, посредством Zwipe, легко можно обеспечить двухфакторную аутентификацию в ЦОД, НИИ, медицинских кабинетах и лабораториях, зонах операций с наличностью, депозитариях, аэропортах, исправительных учреждениях, где годами эксплуатируются традиционные средства ограничения доступа. При этом, как сказано выше, это не потребует каких-либо инвестиций в инфраструктуру, квалификационных тренингов или привлечения IT-ресурсов. Помимо классических СКУД, новому продукту можно найти и ряд других сфер применения: правительственные и социальные проекты, VIP-карты, карты лояльности в сфере услуг, персональные медицинские записи и т.д.

Варианты применения ограничены только фантазией заказчика или интегратора

БИОМЕТРИЧЕСКИЕ КАРТЫ ZWIPE: ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

Как данные об отпечатке пальцев сохраняются на карте?
При регистрации отпечатка сенсор отправляет дактилоскопические данные на процессор Zwipe. Запатентованный алгоритм создает цифровой шаблон, или точнее хешированный дактилоскопический образ, и сохраняет его в постоянной энергонезависимой памяти процессора. Данные в процессоре блокируются для гарантии конфиденциальности прошивки и шаблона.
Поскольку цифровой шаблон – это часть запатентованного алгоритма хеширования отпечатков Zwipe, он не имеет ценности для любого другого дактилоскопического приложения.

Каким образом устанавливается РЧ-коммуникация между считывателем и картой Zwipe?
РЧ-коммуникация между транспондером карты и считывателем заблокирована до тех пор, пока не пройдена успешная биометрическая аутентификация. Радиочастотная сессия длится ровно столько, сколько палец авторизованного пользователя находится на сенсоре карты. Когда палец снят с сенсора, коммуникация со считывателем прекращается.

Взаимодействует ли процессор Zwipe со встроенным транспондером?
Биометрическая регистрация и аутентификация на 100% независимы от интегрированного транспондера (чипы Prox или Mifare). Таким образом, между ними не существует никакой связи.

Есть ли необходимость в сторонних устройствах регистрации отпечатков или API?
Нет, весь процесс регистрации отпечатков пальцев выполняется напрямую с карты. Карта не транслирует никаких биометрических данных на внешние устройства.

Можно ли считать/записать информацию в бесконтактный чип после регистрации отпечатка пользователя?
Да, после успешной биометрической аутентификации, между транспондером и считывателем устанавливается стандартная радиочастотная сессия на время, пока палец пользователя находится на сенсоре. Новое приложение может быть загружено на чип, а существующее сегменты/данные – модифицированы (Mifare).

Можно ли удалить цифровой шаблон?
В целях безопасности удалить или изменить шаблон зарегистрированного отпечатка невозможно.

Сколько времени занимает процесс регистрации отпечатка?
Менее 60 секунд.

Сколько времени занимает процесс аутентификации?
Менее 1,5 секунд.

Как внести карту в базу данных и ПО системы контроля доступа?
До создания цифрового шаблона, серийный номер или сайт-код транспондера может быть легко считан существующим считывателем инициализации карт и внесен в СКУД. После этого пользователь регистрирует свой палец на карте тем самым блокируя память от внешнего доступа.

Блокируется ли карта после нескольких неудачных попыток аутентификации?

Карта позволяет сделать до 4 неудачных попыток аутентификации после чего переходит в спящий режим. Процесс аутентификации может быть возобновлен немедленно нажатием емкостной кнопки на устройстве. В карте не предусмотрена постоянная блокировка при неверной аутентификации.

Срок эксплуатации элемента питания?

В картах Zwipe используются стандартные заменяемые батареи CR2032, свободно доступные в любом магазине электроники. Батарея рассчитана на 4000 циклов аутентификации, что в зависимости от интенсивности эксплуатации гарантирует работу на протяжении от 1 до 2 лет. Рекомендуется заменять элемент питания один раз в год. При низком заряде батареи яркость зеленого светодиода во время аутентификации заметно снизится. Карта может использоваться еще некоторое время, давая пользователю возможность заменить элемент питания. При полном разряде батареи оба светодиода перестают функционировать. В этом случае необходимо просто установить новую батарею.

Что произойдет если извлечь батарею?

Поскольку дактилоскопический шаблон хранится в энергонезависимой памяти, извлечение батареи не приведет к его повреждению или удалению.

Тамперная защита

Карты Zwipe защищены от стороннего вмешательства посредством использования комбинации из специальной водозащитной прокладки и внутренних замков корпуса. Попытки открыть карты приведут к разрушению замков, что может служить доказательством вскрытия корпуса.

Насколько долговечна карта?

Эксплуатируйте карту Zwipe с большими предосторожностями. Это гарантирует годы надежной работы. Карты устойчивы к грязи, жиру, конденсату или случайному падению, к водяным брызгам (не к погружению под воду) и стабильно работают в диапазоне температур от -20°C до +40°C. Сенсор протестирован на 10 млн. циклов сканирования и имеет защитное покрытие, предотвращающее появление царапин на его поверхности.

Гарантия

Zwipe гарантирует отсутствие заводских дефектов в нормальных условиях эксплуатации и при должном обслуживании на протяжении 12 месяцев. Гарантией не покрываются карты, содержащие следы физического, климатического или электрического воздействия.

Можно ли персонализировать карты?

Да, на заднюю крышку карты можно наклеить большинство этикеток стандарта Clamshell с информацией о пользователе с/без прорези под шнурок.

Содержат ли карты внешний идентификационный номер?

Карты содержат серийный номер (не имеет отношения к CSN или сайт-коду транспондера).

Комплексные решения для систем безопасности

WWW.STA.COM.UA