ПЕРЕВОД СКУД С КАРТ EM MARIN НА КАРТЫ MIFARE®

ПОЛЕЗНЫЕ СВЕДЕНИЯ ДЛЯ ВЛАДЕЛЬЦА ОБЪЕКТА СКД

О. Быков
к.т.н., генеральный директор, компания NCS

Подавляющее большинство современных систем контроля доступа (СКД) использует в качестве средств доступа идентификаторы, работающие на частоте 125 кГц. Это проксимити карты доступа (только чтение), самыми распространенными являются карты Em Marin, а также HID, Indala.

Карты этого стандарта являются удобным средством открывания дверей и турникетов. Но, не более. Эти карты не обладают никакой защищенностью, легко копируются и подделываются и, соответственно, ничего не дают для защиты объекта от несанкционированного проникновения.

А именно это зачастую и требуется от современных систем контроля доступа – предотвращение несанкционированного доступа на территорию объекта или в помещение.

Настоящую защиту от копирования и подделки обеспечивают такие идентификаторы, в чипах которых реализована криптографическая защита. Это бесконтактные смарт-карты, работающие на частоте 13,56 МГц, наиболее распространенными из них являются карты Mifare®, HID iClass. В картах этих стандартов криптозащита организована на высоком уровне, и подделка таких карт практически невозможна.

В данной статье рассматривается простой и легкий путь замены карт доступа Em Marin на действующем объекте СКД на карты стандарта Mifare®.

Планируя замену карт Em Marin на карты Mifare® в действующей СКД (или выбирая стандарт Mifare® в качестве карт доступа для новой СКД), следует уделять особое внимание процессу выпуска карт доступа. В отличие от обычного Em Marin, бесконтактные смарт-карты имеют память для записи-чтения и механизм криптографической защиты от несанкционированного чтения или записи данных в чип карты. И для того, чтобы в полной мере использовать имеющиеся возможности, заказчик СКД должен организовать у себя на объекте определенную процедуру выпуска карт доступа.

Основные отличия карт Mifare® и Em Marin приведены *в таблице*.

Одно их главных отличий Mifare® от Em Marin – это наличие памяти для многократного чтения-записи. Причем, операции как чтения, так и записи в каждый сектор могут быть защищены крипто-ключами.

I. ТИПИЧНЫЕ ОШИБКИ ПРИ ИСПОЛЬЗОВАНИИ КАРТ ДОСТУПА MIFARE®

Ошибка 1. *Считывание серийного номера карты.*

Если считыватель, установленный у турникета, шлагбаума или двери в помещение будет считывать серийный номер чипа карты Mifare®, то никакого преимущества по сравнению с картами Em Marin достигнуто не будет. Затраты на более дорогие карты доступа будут напрасными. Серийный номер чипа Mifare® (UID) можно скопировать, хоть и несколько сложнее, чем UID карты Em Marin. При считывании серийного номера Mifare® никак не задействуются криптографические функции, а это означает работу на уровне Em Marin, без защиты карты от копирования.

Чтобы правильно использовать функциональные возможности карт Mifare® надо

Табл. 1

	Mifare® 1K	Mifare® Plus	Em Marin
Частота	13,56 МГц	13,56 МГц	125 кГц
Серийный номер, всегда открытый для считывания	да, длиной 4 байта	да, длиной 7 байт	да, длиной 3 байта
Режим работы	чтение-запись	чтение-запись	только чтение
Структура памяти	16 секторов	до 64 секторов	отсутствует
Защита операций чтения и записи	ключ к чтению каждого сектора	ключ к чтению каждого сектора	отсутствует
	ключ к записи в каждый сектор	ключ к записи в каждый сектор	
Криптографический алгоритм	CRYPTO-1	3 DES	отсутствует

считывать не серийный номер чипа, а данные из некоторого блока памяти карты (secure sector), доступ к которому защищен криптоключами.

Ошибка 2. *Подключения считывателя по Wiegand-26.*

Ситуацию, когда с карты Mifare® считывается серийный номер, а сам считыватель подключается к контроллеру через интерфейс Wiegand-26, можно назвать типичной. Но неправильной.

Обусловлено это тем, что в подавляющем большинстве современных СКД считыватели карт подключаются по интерфейсу Wiegand, и чаще всего по его конкретной реализации – Wiegand-26. И монтажник думает, что подключив вместо считки Em Marin считку Mifare®, он переведет действующую СКД на более высокий уровень защищенности.

Не переведет.

Ошибка в подключении считок Mifare® по интерфейсу Wiegand-26 (для чтения серийного номера) заключается в том, что номер UID Mifare® будет передаваться не полностью. Длина серийного номера Mifare® 1K – 4 байта. А по Wiegand-26 передается только 3 байта. Эта ошибка приводит к появлению в системе дубликатов номеров карт.

Для того, чтобы полностью считывать UID Mifare®, надо подключать считыватели по интерфейсу Wiegand-42 (который позволяет передать в контроллер все 4 байта серийного номера Mifare®).

II. КАК ЗАМЕНИТЬ КАРТЫ EM MARIN НА КАРТЫ MIFARE®

Для того, чтобы в действующей СКД заменить карты Em Marin на карты Mifare®, необходимо выполнить простые действия:

1) Идентификатор карты Em Marin записать в память карты Mifare® *(рис. 1)*.
2) Настроить считыватели Mifare® на чтение того блока памяти, в который записан идентификатор Em Marin.
3) Заменить считыватели Em Marin на считыватели Mifare® *(рис. 2)*.

Все остальное сохраняется: программное обеспечение, база данных, отчеты и т.п. Проходы по новым картам Mifare® будут обрабатываться точно так же, как и по старым картам Em Marin.

Но выполнение этих трех, перечисленных выше этапов характеризуется определенными тонкостями. Рассмотрим эти этапы подробнее.

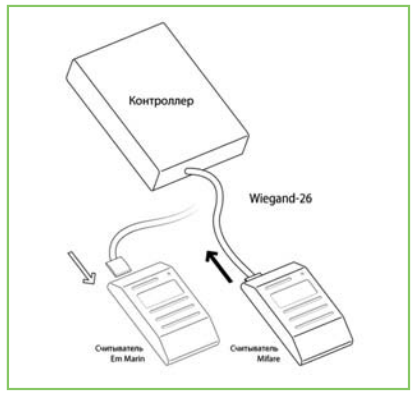


Рис. 2

1. ЭМИССИЯ КАРТ

Эмиссия – это такой этап, обратить внимание на который должен сам владелец объекта с установленной СКД.

Когда владелец объекта может быть уверен в том, что карты, открывающие доступ в важные помещения, не будут подделываться? Только тогда, когда защиту от подделки он продумает и реализует самостоятельно (или через свое доверенное лицо). Нельзя передавать эти функции разработчику или установщику СКД.

Если сразу после закупки карты доступа Mifare® будут выдаваться работникам – это ошибка. Для того, чтобы использовать все преимущества карт Mifare®, их нужно подвергнуть двум процедурам, которые отсутствуют при использовании карт Em Marin, а именно – пред-эмиссии и эмиссии.

1.1. Пред-эмиссия. Запись ключей (прошивка карт Mifare®)

Первое, что владелец объекта должен сделать, – это выбрать один сектор или несколько секторов памяти Mifare®, в которых будут храниться данные. Второе – придумать значения ключа А для доступа к выбранным секторам памяти Mifare®. В дальнейшем значение ключа А должно надежно храниться в сейфе.

Во все закупленные карты Mifare® записывается ключ А.

В результате проведенной пред-эмиссии карты Mifare® оказались переведенными из открытого заводского состояния в закрытое и защищенное состояние для данного объекта СКД *(рис. 3)*.

1.2. Запись идентификаторов Em Marin в память карты Mifare®

Действующая карта доступа Em Marin изымается у работника.

Идентификатор (серийный номер чипа) карты Em Marin записывается в сектор карты Mifare® (в тот сектор: который выбран на этапе пред-эмиссии).

Карта доступа Mifare® выдается работнику.

Эти действия производятся со всеми картами Em Marin, находящимися на руках у работников, до тех пор, пока не будут заменены все имеющиеся карты Em Marine *(рис. 4)*.

2. НАСТРОЙКА СЧИТЫВАТЕЛЕЙ

Для того, чтобы считыватели могли работать с картами Mifare®, прошитыми на предыдущем этапе, в них должны быть загружены соответствующие ключи. Не все считыватели подходят для работы в таком защищенном режиме, на что также следует обратить внимание владельцу объекта. Для использования в защищенном режиме подходят только такие считыватели Mifare®, которые могут хранить в своей энергонезависимой памяти ключи для доступа ко всем 16 секторам Mifare®. Многие дешевые считыватели не обладают такой характеристикой и, соответственно, бесполезны для защищенной СКД.

Запись ключей в считыватели Mifare® переводятся с помощью специальной мастер-карты или карты-конфигуратора.

Карта конфигурации подносится к каждому считывателю. В результате все считыватели переводятся из открытого заводского состояния в защищенное состояние, в котором они смогут работать с «прошитыми» картами данного объекта доступа.

3. ЗАМЕНА СЧИТЫВАТЕЛЕЙ

Считыватели Em Marin, установленные у турникетов, дверей и т.п., демонтируются. Вместо них устанавливаются уже «прошитые» считыватели Mifare® и подключаются к контроллерам по интерфейсу Wiegand-26 *(рис. 3)*.

Рис. 1

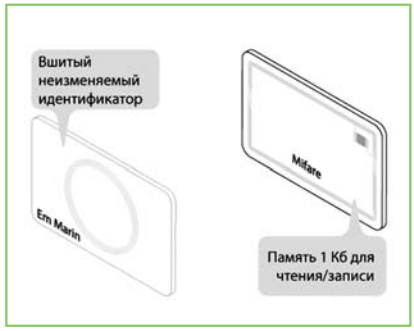


Рис. 3

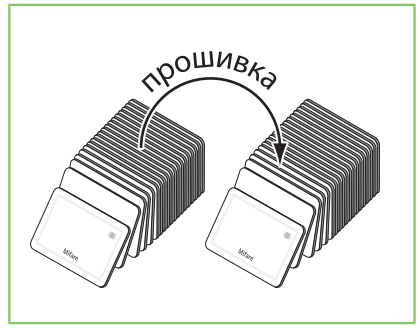
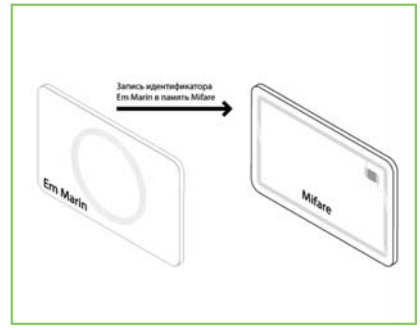


Рис. 4



4. ФУНКЦИОНИРОВАНИЕ СКД ПО КАРТАМ MIFARE®

Все карты Em Marin заменены на «прошитые» карты Mifare®. Вместо старых считок Em Marin к контроллерам (по Wiegand-26) подключены считки Mifare®. Эти считки читают данные из защищенного блока памяти Mifare® (secure sector), и в контроллер передается такой же идентификационный номер, который был у старой карты Em Marin.

Никаких других изменений, кроме отмеченных выше, не требуется. Проход по новой карте Mifare® фиксируется точно также, как и по старой карте Em Marin. С карты Mifare® считывается такой же идентификационный номер, который был на карте Em Marin. По этому номеру работник однозначно идентифицируется в базе данных.

5. ВЫДАЧА НОВЫХ КАРТ ДОСТУПА MIFARE®

После того, как были заменены все старые действующие карты доступа Em Marin, новым работникам должны выдаваться новые карты Mifare®.

В карты, прошедшие пред-эмиссию на первом этапе, а именно – в выбранный закрытый сектор, производится запись новых идентификационных номеров. Диапазон этих идентификаторов выбирается системным администратором с учетом уже имеющихся номеров, чтобы избежать появления одинаковых номеров в системе.

После этого карты доступа Mifare® можно выдавать работникам.

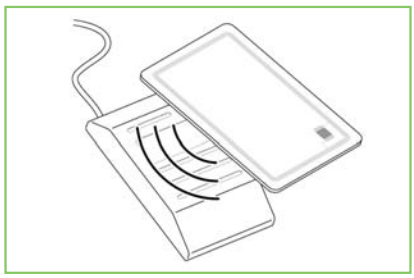
Выдача новых карт доступа Mifare® производится точно так же, как выдавались карты Em Marin (в бюро пропусков или в другом аналогичном месте).

Вместо контрольного считывателя Em Marin к компьютеру подключается контрольный считыватель Mifare® (по интерфейсу USB), который считывает данные из защищенного блока памяти Mifare®. Все остальное происходит точно так же, как и при выдаче карт Em Marin. Идентификатор, записанный в защищенный блок памяти Mifare®, считывается с карты и сохраняется в базе данных вместе с персональными данными работника.

III. КАК ПРАВИЛЬНО ВЫБИРАТЬ КАРТЫ MIFARE®

В отличие от карт EM Marin карты Mifare® представляют собой более сложный продукт, и к закупке таких карт надо подходить более ответственно.

Рис. 5



На что же следует обращать внимание при заказе карт данного стандарта? На качество, которое складывается из следующих составляющих:

- чип карты;
- антенна;
- соединение чипа и антенны.

Рассмотрим подробнее:

1. ЧИП КАРТЫ

Чипы Mifare® 1K бывают оригинальные и нет. От этого зависят такие параметры, как надежность и корректность работы с памятью чипа.

Карты Mifare® 1K были изначально разработаны фирмой Philips и предназначались для локальной оплаты на транспорте. В настоящее время все проекты Mifare® ведет дочерняя фирма Philips – компания NXP Semiconductors.

Чип от NXP называется MF1 IC S50 и является самым правильным «оригинальным» чипом.

Кроме NXP, оригинальные чипы выпускает фирма Infineon на основании лицензии от NXP. Чип от Infineon называется SLE66R35. По надежности и другим параметрам данный чип ничем не отличается от чипа NXP.

Название MIFARE – торговая марка семейства бесконтактных смарт-карт, принадлежащая NXP Semiconductors.

Все продукты MIFARE® базируются на международном стандарте ISO 14443 Type A – стандарте бесконтактных смарт-карт. Чипы, совместимые с Mifare® 1K, также разработаны на основе данного стандарта ISO.

На рынке существуют чипы, кроме MF1 IC S50 и SLE66R35, которые называют «совместимые» или «неоригинальные» чипы Mifare® 1K. Но, так как эти чипы выпускаются без лицензии NXP, носить название Mifare® на законных основаниях они не могут. Фирмы-разработчики таких чипов этого и не делают, они дают своим чипам другие названия. А словосочетание «совместимый Mifare» или «неоригинальный Mifare» придумали менеджеры по продажам.

Из таких совместимых чипов наиболее известными являются:

- FM11RF08/Fudan;
- BL75R06/Belling;
- IS4439/ ISSI;
- SHC1102/ HuaHong и др.

Заводы-изготовители таких чипов в своей технической документации, естественно, не упоминают Mifare®, а ссылаются на стандарт ISO 14443 Type A.

Следует иметь в виду, что стоимость совместимых чипов значительно ниже, чем стоимость оригинальных.

Есть еще такое понятие, как корректная или полная реализация стандарта ISO 14443 Type A. Не все совместимые чипы обладают такой реализацией. Это означает, что при выполнении сложных функций по операциям с памятью «Mifare-совместимого» чипа, такие чипы могут работать неправильно. Что и происходит на практике. Заказчик, польстившись на низкую стоимость, с удивлением обнаруживает, что карты через некоторое время перестают работать.

2. АНТЕННА

Бесконтактные смарт-карты стандарта ISO 14443 Type A работают на частоте 13,56 МГц. Т.е. и считыватель, и карта должны обеспечить работу на частоте 13,56 МГц. Для этого внутри карты имеется антенна. Чаще всего антенна делается из нескольких витков медной проволоки. Медная проволока может наматываться китайским рабочим вручную, а может наматываться на автоматическом станке. При намотке на станке антенна получается идеально ровной, чего нельзя сказать о ручной намотке. От этого может зависеть реальная частота, на которой данная антенна будет работать, и, соответственно, дальность считывания и правильность передачи данных между картой и считывателем.

3. СОЕДИНЕНИЕ ЧИПА И АНТЕННЫ

Чип и антенна должны быть надежно соединены. Иначе не будет передачи данных между картой и считывателем. От качества этого соединения зависит надежность и долговечность работы карты. Если площадь контакта антенной проволоки и чипа достаточно велика и качество пайки (сварки) высокое, карта будет долго и безупречно работать. Высокотехнологичные производства это обеспечивают.

Но если все делается вручную, обычным паяльником, со слабым технологическим контролем, то соединение чипа с антенной может оказаться слабым и разрушиться при использовании карты (от небольших вибраций и других внешних воздействий).

Вот три наиболее важных момента, которые следует иметь в виду при заказе бесконтактных смарт-карт Mifare®.

Примечание: Об оригинальности чипов Em Marin и Mifare®.

То, что в народе называется Em Marin, представляет собой самую популярную карту доступа EM4102 от швейцарской фирмы EM Microelectronic-Marin SA. Но оригинальные чипы EM4102 практически отсутствуют на рынке. Подавляющее большинство карт доступа (браслетов, брелоков) поставляется с китайским аналогом TK4100 (и, строго говоря, называться Em Marin не может).

Mifare® – это торговая марка фирмы NXP Semiconductors. Никто, кроме NXP, не может использовать для своих чипов (на законных основаниях) наименование Mifare.

В Китае производятся «совместимые» чипы. Но заводы-изготовители их и не называют Mifare, а дают свои наименования (например, ISSI, F08, TKs, HuaHong).

К сожалению, на отечественно рынке многие поставщики не делают такой дифференциации и поставляют «совместимые» чипы, как настоящие Mifare®.

IV. Как добавить в СКД доступ по отпечаткам пальцев

Дополнительно повысить защищенность и безопасность СКД можно, добавив предоставление доступа по карте + по отпечаток пальца.

Если такое повышение статуса СКД необходимо для системы, где уже есть карты Em Marin, то, вместе с заменой карт Em Marin на карты Mifare можно легко и просто добавить верификацию по отпечатку пальца. Выполняется это с помощью комбинированного считывателя Mifare и отпечатка пальца, который подключается к контроллеру по интерфейсу Wiegand-26.

Считыватель работает следующим образом. Вначале считывается карта Mifare, в памяти которой хранится отпечаток пальца владельца карты. Затем сканируется палец. Считыватель сравнивает оба отпечатка и при совпадении посылает в контроллер идентификационный номер, записанный в защищенном секторе MIfare.

V. Заключительные замечания

В заключение перечислим основные моменты, на которые следует обращат внимание владельцу объекта СКД.

1) Вместо считывания серийного номера чипа, надо считывать данные из защищенного блока памяти карты Mifare. Длина данных, записанных в блок памяти, должна быть не более 3 байт, чтобы полностью передать по Wiegand-26.
2) Не рекомендуется использовать карты Mifare сразу после покупки. Пользователю следует поменять открытые заводские ключи на свои собственные,секретные ключи. Если не использовать ключи при работе с продуктами Mifare, то нет смысла и в самих картах Mifare. В этом случае дешевле и проще применять Em Marin. Все преимущества продуктов Mifare будут реализованы только тогда, когда пользователь будет закрывать доступ к чтению-записи данных из чипа Mifare по своим секретным ключам. И будет делать это самостоятельно, а не получать от поставщика карту с уже записанными (и неизвестными пользователю) ключами.
3) Правильно использовать такие считыватели, которые хранят в своей энерго-независимой памяти ключи доступа к секторам памяти Mifare. Если ключи доступа хранятся не в считывателе, а в компьютере, – то они легко могут быть скопированы.
4) Владелец системы (доступа, оплаты, и т.п.) должен предусмотреть два этапа выпуска карт:

- пред-эмиссия;
- эмиссия.

Пред-эмиссия нужна для того, чтобы перевести карты Mifare с открытого заводского уровня на защищенный уровень, принятый в данной системе. С завода-изготовителя карты Mifare поступают открытыми и незащищенными.

Очень важно для владельца объекта СКД знать, что закупаемые им карты Mifare находятся на открытом заводском уровне и никакая информация в память карты не записана. Иногда поставщики карт Mifare самостоятельно (и без ведома заказчика) прописывают свои ключи в карты Mifare, защищая их якобы от подделки. Это неправильно. Поставщик привязывает таким образом владельца СКД к своим картам. А, зная значение ключей, он имеет все возможности для взлома и подделки карт.

Генерировать ключи и записывать их в карты должен сам владелец объекта, на котором установлена СКД, или его доверенное лицо.