ЭРА НОВЫХ ТЕХНОЛОГИЙ

ДОСТУП ПОД КОНТРОЛЕМ

www.entpro.ru

Руководство по эксплуатации считывателя бесконтактных карт ЭРА-MF

Сделано в России

Редакция от 03.12.2024

Оглавление

Условные обозначения, принятые в руководстве

–этой меткой будет обозначена критически важная информация. Если не соблюдать правила и условия, описанные в разделах, помеченных этой меткой, система не будет работать.

– абзацы, выделенные данным знаком, составляют важную информацию о системе, которая облегчит работу с ней.

– справочная информация, разъясняющая некоторые понятия системы.

Список принятых сокращений

СКУД – Система контроля и управления доступом.

ОС – Операционная система.

ПО – Программное обеспечение.

ПК – Персональный компьютер.

UID ключа – Уникальный идентификатор ключа.

1. Общее описание считывателя ЭРА-MF

Комплектация:

1) Считыватель Эра-MF
2) Паспорт изделия
3) Плата управления замком LBRD 1.0 (комплектация Эра-MF+)

Формат идентификаторов:

1) ISO14443A:
   - Чтение UID 4/7 байт карт стандарта Mifare;
   - UID 8 байт телефона с NFC (Android);
   - Чтение закрытых областей карт Mifare Classic, Mifare Plus S, Mifare Plus SE и Mifare Plus X.
1) UID 4 байта ISO14443B;
2) UID 8 байт ISO15693 (ICODE).

1.1. Режимы работы считывателя ЭРА-MF

1) Незащищенный режим (без шифрования) - чтение UID ключа и/или телефона (только для ОС Android);
2) Защищенный режим (с шифрованием):
   - Режим «Код Объекта»;
   - Режим «Чтение кода из блока»;
   - Режим «Зоны прохода».

1.2. Световая и звуковая индикация считывателя ЭРА-MF

Индикация может работать по внутренней или внешней логике. При включении считыватель работает по внутренней логике. В случае, если был подан управляющий сигнал на контакты *LedG*, *LedR* или *Beep*, то считыватель переходит в режим управления внешними сигналами.

Работа индикации при управлении внешними сигналами предусматривает 4 цветовых режима:

1) Отсутствие управляющих сигналов на *LedG* и *LedR* (по умолчанию «синий»);
2) Присутствует только сигнал *LedG* (по умолчанию «зеленый»);
3) Присутствует только сигнал *LedR* (по умолчанию «красный»);
4) Присутствуют оба сигнала *LedG* и *LedR* (по умолчанию «оранжевый»);

Цвета по умолчанию могут быть изменены с помощью ПО. Возможно как поменять цвет, так и отключить индикацию в данном режиме вообще, выбрав черный. Данные изменения коснутся работы индикации как по внутренней, так и по внешней логике. Например, при работе по внутренней логике в режиме ожидания горит индикация «Режим 3». При успешном чтении включается «Режим 2» и т. д.

2. Подробное описание режимов работы считывателя

2.1. Защищенный режим: код объекта

Данный режим является защищенным. Это означает, что идентификация карт будет происходить не по UID ключа, а по информации, содержащейся в определенной области, закрытой от чтения секретным ключом. В данном режиме возможно использование одного из двух типов карт:

1) Mifare Classic 1K или 4K, (Mifare ID не подойдет);
2) Mifare Plus (SE, S, X).

Поддержка Mifare Classic сделана исключительно для возможности использования в существующих системах, где уже имеется определенное количество карт в обороте и требуется повысить уровень безопасности. Следует понимать, что на текущий момент карты Mifare Classic нельзя считать безопасными, так как их можно копировать. Однако сделать это сложнее (дороже, хоть и незначительно), чем скопировать UID. Для сравнения Mifare Classic и Mifare Plus можно привести следующую таблицу:

	Mifare Classic	**Mifare Plus**
Алгоритм шифрования	Crypto1	AES
Длинна ключа, бит	48	128

Для исключения возможности копирования карт, особенно при проектировании новых объектов, следует использовать карты стандарта Mifare Plus. Самые простые и, как следствие, доступные по цене – это карты Mifare Plus SE 2K. Карты большей емкости и стандартов Plus S и Plus X также могут быть успешно использованы в данном режиме.

Для данного режима следует использовать карты, нигде ранее не использованные и находящиеся в так называемом «транспортном состоянии» (в этом состоянии находятся карты при выходе с завода-изготовителя). Этот момент важен, так как система конфигурирует карты самостоятельно и переводит их из «транспортного состояния» в режим SL3. Карты, переведенные в режим SL1, SL2, SL3 считывателями

другого производителя использоваться в данном режиме уже НЕ смогут (т.к. при этом будут использованы неизвестные системе коды доступа, а перевод обратно в транспортный режим невозможен)! Также следует отметить, что при переводе считывателем карт в режим SL3 устанавливается Random UID. Т. е. карта будет выдавать каждый раз разный UID размером 4 байта при поднесении к считывателям, работающим только по UID. Это позволяет «обезличить» бесконтактные карты для любых сторонних систем. Как в случае Mifare Classic, так и в случае Mifare Plus используется механизм диверсификации ключей. Это означает, что в каждой бесконтактной карте будут свои ключи для доступа к закрытым областям, что также положительно сказывается на защищенности системы. Подбор ключа для одной карты позволит скопировать только данную карту и не будет действителен для других карт.

Использование данного режима начинается с создания мастер-карт с кодом объекта.

Для создания мастер-карт мы рекомендуем использовать карты Mifare Plus. Тем не менее, вы можете воспользоваться и картами Mifare Classic, но стоит учесть, что они не являются некопируемыми, а значит, существует риск их копирования.

Если вы используете защищённый режим код-объекта на основе Mifare Plus, то применение мастер-карт Mifare Classic становится невозможным.

Всего мастер-карт с одинаковым кодом можно создать не более 5 штук. Все они создаются за один раз и нумеруются. Т. е. на каждой карте содержится информация, сколько таких карт было создано и какой номер по порядку у данной карты. При чтении конфигурации с мастер-карты в заголовке всплывающего окна вы можете получить информацию о том, сколько было создано карт с такими настройками. Это важно, если после развертывания системы заказчики захотят убедиться, что им были отданы все карты с кодом именно их объекта.

Код объекта формируется как случайное число при создании мастер-карты и содержится **только на мастер-картах, созданных единовременно** (до 5-ти мастер-карт). Посмотреть код объекта, переписать его куда либо, принудительно **создать другую мастер-карту** (кроме уже созданных) **с таким кодом невозможно!** Помимо кода объекта, мастер-карта содержит и другие настройки, которые фигурируют на вкладке данного режима. Мастер-карты могут быть использованы для дальнейшего конфигурирования считывателей с одинаковыми настройками на объекте без использования программы для ПК. С мастер-карты возможно считать настройки, кроме закрытых. Например, вместо кода объекта вы получите контрольную сумму кода объекта. Это позволит вам в случае необходимости определить, какие мастер-карты

содержат одинаковый код объекта (у них будут одинаковые контрольные суммы), но **в оригинальном виде код объекта вы посмотреть не сможете**.

В защищенном режиме «код объекта» на каждую карту пользователя записывается код объекта. Аналогичный код объекта записывается и в считыватели на этапе конфигурации. При прикладывании карты считыватель, обращаясь к закрытой области, ищет там соответствующий код объекта. Если код найден, то считыватель выдает ID карты. Если код не найден или не соответствует, то ничего не происходит. Каждая карта пользователя может содержать более 10 различных кодов объектов, что позволяет использовать одну и ту же карту на разных объектах.

Карты, которые были отформатированы данной системой, могут быть использованы повторно, т. е. с карты можно удалить всю информацию с конфигурацией (стереть мастер-карту) и использовать ее как карту пользователя, записав туда код объекта, и наоборот. Также с карты пользователя можно удалить конкретный код объекта (при наличии мастер-карты с этим кодом) или все коды объектов сразу. Данные возможности позволяют повторно использовать карты или даже менять коды объекта системы в процессе эксплуатации, если это необходимо.

На этапе создания мастер-карт можно использовать опцию настроек, при которой вы не сможете переконфигурировать считыватель другой мастер-картой (картой, у которой другой код объекта). Это возможно сделать только той картой (картами с одинаковым кодом объекта), с помощью которой он был переведен в данный защищенный режим. Эта функция позволяет избежать несанкционированного переконфигурирования системы.

Подробное описание настройки системы в режиме «**код объекта**» указано в «**Руководстве пользователя ЭНТ Контроль Доступа – RFID**».

2.2. Защищенный режим: чтение кода из блока

Данный режим предусмотрен для случаев, когда на объекте уже существует своя система с картами Mifare Plus в режиме SL3. В этом случае вы можете использовать как идентификатор информацию в закрытой области памяти карты. Для этого вам нужно указать номер блока, смещение в данном блоке и количество байт для передачи. Максимальное количество байт для передачи – **8**. Также вам требуется указать код доступа к данному блоку. Размер кода доступа **16** байт. В данном режиме код доступа вводиться в открытом виде и его следует беречь от «чужих глаз», так как он может быть легко скопирован для создания дубликатов карт и других нарушений. Как и в

предыдущем защищенном режиме возможно создать до 5 мастер-карт с настройками. При чтении настроек с мастер-карты пользователю будет выводиться контрольная сумма кода доступа к блоку, чтобы исключить его несанкционированное копирование.

Подробное описание настройки системы в режиме «**чтение кода из блока**» указано в «**Руководстве пользователя ЭНТ Контроль Доступа – RFID**».

2.3. Защищенный режим: зоны прохода

В этом режиме считыватель ЭРА-MF выполняет функцию контроля доступа. Отличительной особенностью такого режима является отсутствие необходимости в базе бесконтактных карт, что в некоторых случаях может быть весьма удобно. Например, этот режим прекрасно подходит для больших жилых комплексов, где ведение БД затруднительно, и часто используются контроллеры в режиме автозаписи. Давайте более подробно рассмотрим особенности этого режима.

При использовании данного режима объект следует разделить на несколько зон, доступ к которым требуется разграничить. Максимальное количество зон – **64**. Как пример, можно рассмотреть жилой комплекс из 20 подъездов, огороженный забором с калитками. Каждый подъезд можно выделить как одну зону, и все калитки также выделить в одну общую зону. Итого в данном примере будет использоваться 21 зона.

Данный режим также, как и первый защищенный режим, использует понятие кода объекта. Код объекта генерируется при создании мастер-карт (от 1 до 5 штук). На этапе конфигурирования системы в считыватели записывается код объекта и соответствующие данному объекту зоны прохода. Таким образом, в нашем примере получится, что у каждого подъезда будут стоять считыватели, у которых будет прописана одна зона, соответствующая конкретному подъезду (например, с 1 по 20). Считыватели на калитках будут иметь разрешенную зону 21.

При формировании карт пользователей оператор может выбрать, в какие зоны будет разрешен доступ обладателю этой карты. В данном примере каждому жителю будет разрешен доступ в две зоны – в его подъезд и калитки. Работникам коммунальных служб можно разрешить доступ во все зоны. При поднесении карты считыватель смотрит, какие зоны записаны на карте, и если хотя бы одна совпадает с зонами, прописанными в нем, то он разрешает проход.

В данном режиме передача данных по протоколу Wiegand, USB не прекращается. Однако передается не идентификационный номер карты, а битовая строка разрешенных зон.

Для удобства администраторов системы в ПО можно переименовать зоны в удобные для использования названия и сохранить эти настройки в шаблонах.

Внимание! *Данный режим работы считывателя ЭРА-MF возможен только при наличии платы LBRD 1.0 (входит в состав ЭРА-MF+).*

*Подробное описание настройки системы в режиме «**Зоны прохода**» указано в «**Руководстве пользователя ЭНТ Контроль Доступа – RFID**».*

3. Дополнительно

2.4. Руководство пользователя ЭНТ Контроль Доступа – RFID

2.5. Программа ЭНТ Контроль доступа – RFID

2.6. Программа ЭНТ Контроль доступа – RFID для Android

2.7. Программа ЭНТ Контроль доступа - NFC Reader.