MIFARE® ID

Техническое описание

1. Общее описание

Смарт-карты MIFARE® ID соответствуют стандарту ISO/IEC 14443 Type A.

Возможные сферы применения смарт-карт MIFARE® ID:

- Системы контроля физического доступа (СКУД) для бизнеса и дома;
- Электронный ключ к номеру в гостинице или камере хранения;
- Карта доступа для парковки, стоянки или гаражного комплекса;
- Программы лояльности, карта постоянного клиента;
- Клубная карта для фитнес-клубов и развлекательных комплексов;
- Карта школьника и студента;
- Интерактивные лотереи и игры;
- Другие проекты, где требуется простая идентификационная карта.

1.1 Антиколлизия

Встроенный механизм антиколлизии позволяет работать с конкретной картой, даже если в зоне действия считывателя находится более одной карты.

1.2 Безопасность

- Уникальный[1] идентификатор карты (UID) размером 4 байта;
- Карты в одной партии могут иметь непоследовательные идентификаторы (по требованию);
- Взаимная аутентификация в три прохода по ISO/IEC DIS 9798-2;
- Возможность задать два ключа доступа.

2. Характеристики и преимущества

- Бесконтактная передача данных;
- Карта получает питание от считывателя;
- Рабочая частота 13,56 МГц;
- Проверка целостности данных CRC 16 бит, бит чётности, побитное кодирование, контроль разрядов;
- Типовое время обработки транзакции <100 мсек, включая резервное копирование данных;
- Неуникальный идентификатор 4 байта;
- Считывание на расстоянии до 100мм в зависимости от считывателя и конструкции антенны;
- Скорость передачи данных 106 кбит/сек;
- Механизм антиколлизии;

[1] Уникальный идентификатор, размером 4 байта, гарантирован для всей серии карт MIFARE® ID. Из-за ограниченной длины может пересекаться с ранее выпущенными картами с 4 байтным идентификатором из семейства MIFARE® Classic и MIFARE® Plus.

- Возможность проверки подлинности чипа (Originality Check)[2].

2.1 EEPROM

- 64 байт в 1 секторе из 4 блоков (один блок составляет 16 байт);
- 32 байта пользовательской памяти;
- Срок хранения данных 10 лет;
- Возможность задать условия доступа к сектору;
- До 200 000 циклов перезаписи.

3. Краткая спецификация

Таблица 1. Краткая спецификация MIFARE® ID

Символ	Параметр	Условия		Мин.	Тип.	Макс.	Ед.
F_i	Частота входного сигнала			-	13.56	-	МГц
Характеристики EEPROM							
T_{ret}	Хранение данных	$T_{окр}$ = 22°C		10	-	-	Лет
endu(W)	Циклов перезаписи	T = 22°C		100 000	200 000	-	Циклов

4. Функциональное описание

4.1 Описание модуля

Смарт-карты MIFARE® ID имеют EEPROM размером 64 байт, РЧ-интерфейс и цифровой блок управления. Энергия и данные передаются посредством антенны, представляющей собой катушку с несколькими витками, подключённую напрямую к чипу смарт-карты MIFARE® ID. Не требуется дополнительных внешних компонентов, например антенн или источника питания.

- РЧ-интерфейс:
  - модулятор/демодулятор;
  - выпрямитель;
  - генератор тактовой частоты;
  - сброс по подаче питания (POR);
  - регулятор напряжения;
- антиколлизия: корректная работа с каждой картой при наличии нескольких карт в зоне действия считывателя;

[2] Подробно описывается в документе NXP AN277210, запрашивается дополнительно после подписания NDA.

- аутентификация: перед выполнением любой операции с памятью проверяется, что имеются два ключа, отвечающие за данный сектор;
- блок хранения значения (VALUE block): данные хранятся в особом формате с избыточностью, для изменения значений используется инкремент и декремент;
- криптографический блок: потоковый шифр CRYPTO1 используется для аутентификации и шифровании при обмене данными.

4.2 Взаимодействие

Считыватель подаёт команды на цифровой блок управления чипа. Ответ на команду зависит от состояния чипа, а для операций с памятью также от того, соблюдены ли условия доступа к указанному сектору.

4.3 Стандартные ответы

После сброса по подаче питания Power-On Reset (POR) карта отвечает на команды REQA или WUPA передачей кода ATR (ATQA по ISO 14443A).

4.3.1 Антиколлизия

При работе со смарт-картой сначала считывается ее идентификатор. Если в поле действия считывателя находится несколько карт, считыватель различает их по идентификаторам и посылает команды только выбранной карте с указанным идентификатором. Выбранная карта указывается в команде Select card. Остальные карты переводятся в состояние ожидания до получения следующего запроса.

4.3.2 Команда выбора карты Select card

Команда Select card предназначена для выбора конкретной карты, с которой будут проводиться операции авторизации и работы с памятью.

Карта возвращает код подтверждения Select AcKnowledge (SAK), который позволяет определить тип выбранной карты.

4.3.3 Трехпроходная аутентификация

После выполнения команды Select card считыватель указывает, к какой области памяти следует обратиться и использует соответствующий ключ для трехпроходной аутентификации (Three pass authentication). После успешной аутентификации все команды и ответы карты передаются в зашифрованном виде.

Примечание: команда HLTA должна передаваться на карту в зашифрованном виде после успешной аутентификации, только в этом случае она будет принята.

4.3.4 Операции с памятью

После аутентификации могут выполняться следующие команды:

- **Чтение** блока;
- **Запись** блока;
- **Декремент**: уменьшение значения блока с сохранением результата во внутреннем буфере;
- **Инкремент**: увеличение значения блока с сохранением результата во внутреннем буфере;

- **Восстановление**: перемещение значения блока во внутренний буфер;
- **Транзакция**: запись содержимого транспортного буфера в блок памяти.

4.4 Целостность данных

Для обеспечения надёжности производимых транзакций при бесконтактном обмене данными используются следующие методы:

- CRC 16 бит на каждый блок;
- Бит чётности на каждый байт;
- Проверка целостности порядка битов;
- Битовое кодирование состояний “1”, “0” и “нет информации”;
- Мониторинг канала.

4.5 Трехпроходная аутентификация. Алгоритм

- Считыватель смарт-карт указывает сектор и выбирает ключ A или ключ B.
- **Проход 1**: Карта считывает секретный ключ и условия доступа из трейлера сектора. Затем карта отправляет считывателю запрос (т.н. challenge).
- **Проход 2**: Считыватель вычисляет ответ на запрос на базе секретного ключа и дополнительных данных. Затем считыватель отправляет на карту ответ на запрос и свой запрос.
- **Проход 3**: Карта проверяет ответ считывателя на свой запрос, отправленный на 1 этапе. Затем карта рассчитывает ответ на запрос считывателя и передаёт его обратно считывателю.
- Считыватель проверяет ответ на запрос, полученный от карты.

После передачи первого запроса на основе произвольных данных, обмен данными между картой и считывателем производится в зашифрованном режиме.

4.6 РЧ-интерфейс

Радиочастотный интерфейс соответствует стандарту для бесконтактных смарт-карт ISO/IEC 14443A.

Для выполнения операций с картой, карта должна находиться в зоне действия считывателя, т.к. излучение считывателя является источником электропитания карты.

При обмене данными в обоих направлениях в начале каждого кадра (фрейма) передаётся только один стартовый бит. Каждый байт завершается битом четности. Первым передаётся младший бит (LSB) байта, т.е. бит с наименьшим адресом в выбранном блоке.

Максимальная длина кадра (фрейма) 163 бита:

16 байт данных + 2 CRC байта = 16 × 9 + 2 × 9 + 1 стартовый бит.

4.7 Организация памяти

Память EEPROM 64 × 8 бит организована в виде одного сектора из 4 блоков. В одном блоке содержится 16 байт.

В первом блоке данных (block 0) первого сектора (sector 0) хранятся данные о производителе чипа и 4-байтный идентификатор.

Блок программируется при производстве чипа и имеет защиту от перезаписи.

Второй и третий блок данных (block 1, block 2) первого сектора (sector 0) используются для хранения данных или значений.

Четвёртый блок данных (block 3) первого сектора (sector 0) называется «трейлер», он содержит по два ключа доступа к каждому блоку и условия доступа.

4.7.1 Блоки данных

Сектор памяти содержит 2 блока (block 1, block 2) по 16 байт для хранения данных. В зависимости от бит доступа каждый блок данных можно сконфигурировать как:

- блок чтения/записи (Read/Write Block);
- блок хранения значения (Value Block).

Блоки хранения значения может использоваться, например, для электронных кошельков. Для блоков хранения данных используются дополнительные команды, например, декремент и инкремент применяются для непосредственного изменения сохранённого значения.

Любая операция с памятью возможна только в случае успешной аутентификации.

Примечание: тип блоков данных по умолчанию не определён.

4.7.2 Блоки хранения значения

Блоки хранения значения (Value block) используются для работы с электронными кошельками при помощи дополнительных функций/операций (доступные команды: чтение, запись, инкремент, декремент, восстановление, транзакция). Блоки хранения значения имеют фиксированный формат, который позволяет обнаруживать возможные ошибки, исправлять неверные значения и управлять резервным копированием данных.

Блок хранения значения можно сконфигурировать только операцией записи в специальном формате.

- **Значение** (Value): значение 4 байта со знаком. Младший бит (LSB) значения хранится в байте с наименьшим адресом. Отрицательные значения хранятся в стандартном формате дополнительного кода (способ представления отрицательных чисел «two's complement»). Для обеспечения надежного хранения и возможности восстановления значения в случае сбоя, значение хранится в памяти 3 раза: два раза в прямом направлении и один раз в обратном.
- **Адрес** (Adr): Адрес размером в 1 байт для хранения адреса блока. Используется для механизма резервного восстановления. Байт адреса хранится четыре раза: два раза в прямом направлении и два раза в обратном направлении. При выполнении команд инкремента, декремента, восстановления и транзакции адрес не изменяется. Адрес может измениться только при выполнении команды записи.

Корректно составленный формат блока хранения значения на примере десятичного значения 1234567d и адреса блока 17d.

Во первых, десятичное значение преобразовывается в шестнадцатеричное 0012D687h. Младший байт шестнадцатеричного значения записывается в Byte 0, старший байт — в Byte 3. Инвертированное представление значения в шестнадцатеричном виде — FFED2978h, Младший байт записывается в Byte 4, а старший байт в Byte 7.

Шестнадцатеричное представление адреса 11h, инвертированное шестнадцатеричное значение EEh.

4.7.3 Трейлер сектора

Трейлером сектора является блок 3, в котором хранятся:

- секретные ключи A (обязательный) и B (опциональный), которые возвращают при чтении логические “0”;
- и условия доступа к блокам данного сектора, которые хранятся в байтах 6...9. Биты доступа также определяют тип блока (данные или хранение значения).

Если ключ B не используется, последние 6 байт трейлера сектора могут использоваться для хранения данных. Для этого необходимо задать биты доступа, как описано в разделе 4.8.2.

В байт 9 трейлера сектора могут быть записаны пользовательские данные. Для байта 9 применяются те же условия доступа, что и к байтам 6, 7 и 8.

При чтении трейлера сектора байты с ключами обрамлены логическими нулями. Если ключ B используется, байты 10-15 могут быть считаны.

По умолчанию для всех ключей новых чипов установлено значение FF FF FF FF FF FF (6 байт FF), а значение байтов 6, 7 и 8 равно FF0780h.

4.8 Доступ к памяти

Перед выполнением любой операции с памятью, карту необходимо выбрать (посредством операции Select card) и провести аутентификацию. То, какие операции можно произвести с блоками памяти, зависит от ключей, предъявленных при аутентификации и от условий доступа, хранящихся в трейлере соответствующего сектора.

Таблица 2. Операции с памятью MIFARE® ID

Операция	**Описание**	**Действительна для типа блока**
Чтение (Read)	Чтение одного блока данных	Блоки чтения записи (read/write block), блоки хранения значения (value block) и трейлеры секторов
Запись (Write)	Запись одного блока данных	Блоки чтения записи (read/write block), блоки хранения значения (value block) и трейлеры секторов
Инкремент (Increment)	Увеличение значения блока с сохранением результата во внутреннем буфере (Transfer Buffer)	блоки хранения значения (value block)

Операция	Описание	Действительна для типа блока
Декремент (Decrement)	Уменьшение значения блока с сохранением результата во внутреннем трансферном буфере	блоки хранения значения (value block)
Транзакция (Transfer)	Запись содержимого внутреннего буфера в блок	Блоки чтения записи (read/write block), блоки хранения значения (value block)
Восстановление (Restore)	Чтение содержимого блока и запись во внутренний трансферный буфер	блоки хранения значения (value block)

4.8.1 Условия доступа

Условия доступа к каждому блоку данных и трейлеру сектора определяют 3 бита, которые хранятся в инвертированном и не инвертированном виде в трейлере сектора.

Биты контроля доступа определяют уровень доступа к памяти по предъявлению секретного ключа A и секретного ключа B. Условия доступа могут быть изменены, если известны действительные ключи и текущие настройки безопасности позволяют осуществить данную операцию.

Примечание: При каждой попытке доступа логический блок чипа проверяет формат задаваемых условий доступа. При обнаружении неверного формата доступ ко всему сектору блокируется без возможности разблокировки.

Примечание: В настоящем описании биты доступа указаны только в прямом порядке (без инверсии).

Логический блок чипа смарт-карты MIFARE® ID гарантирует, что операции с памятью могут быть выполнены только после успешной аутентификации.

Таблица 3. Условия доступа к памяти MIFARE® ID

Биты доступа	Доступные команды	Блок	Описание
$C1_3$, $C2_3$, $C3_3$	read, write	3	Трейлер сектора
$C1_2$, $C2_2$, $C3_2$	read, write, increment, decrement, transfer, restore	2	Блок данных
$C1_1$, $C2_1$, $C3_1$	read, write, increment, decrement, transfer, restore	1	Блок данных
$C1_0$,$C2_0$, $C3_0$	read, write, increment, decrement, transfer, restore	0	Блок данных

4.8.2 Условия доступа к трейлеру сектора

В зависимости от состояния битов доступа к трейлеру сектора (блок 3) доступ на чтение и запись может быть определён как ‘never’ (нет доступа), ‘key A’ (ключа A), ‘key B’ (ключ B) или key A|B’ (ключ A или ключ B).

Сразу после поставки условия доступа к трейлеру сектора и ключи A по умолчанию известны и записаны на карту, это называется транспортной конфигурацией. Поскольку ключ B в транспортной конфигурации может быть считан при предъявлении ключа A, аутентификация новых карт требует предъявления ключа A.

При персонализации карт необходимо учитывать, что при обращении к памяти в неверном формате возможность изменения битов доступа также может оказаться заблокированной.

Таблица 3. Условия доступа к трейлерам секторов MIFARE® ID

Биты доступа			Условия доступа						Примечание
			Ключ А		Биты доступа		Ключ Б		
C1	C2	C3	Чтение	Запись	Чтение	Запись	Чтение	Запись	
0	0	0	Нет	Ключ А	Ключ А	Нет	Ключ А	Ключ А	Ключ В может быть считан *
0	1	0	Нет	Нет	Ключ А	Нет	Ключ А	Нет	Ключ В может быть считан *
1	0	0	Нет	Ключ В	Ключ А|В	Нет	Нет	Ключ В	
1	1	0	Нет	Нет	Ключ А|В	Нет	Нет	Нет	
0	0	1	Нет	Ключ А	Ключ А	Ключ А	Ключ А	Ключ А	Ключ В может быть считан *, транспортная конфигурация
0	1	1	Нет	Ключ В	Ключ А|В	Ключ В	Нет	Ключ В	
1	0	1	Нет	Нет	Ключ А|В	Ключ В	Нет	Нет	
1	1	1	Нет	Нет	Ключ А|В	Нет	Нет	Нет	

* Условия доступа к ключу В позволяют чтение блока, при таких условиях доступа вместо ключа могут быть записаны данные

4.8.3 Условия доступа к блокам данных

В зависимости от битов доступа к блокам данных (блоки 0...2) условия чтения/ доступ на чтение и запись может быть определён как ‘never’ (нет доступа), ‘key A’ (ключа А), ‘key B’ (ключ В) или key A|B’ (ключ А или ключ В). Устанавливать биты доступа следует в зависимости от приложения на карте и необходимости в возможности выполнения определённых команд.

- **Блоки чтения/записи** (Read/write block): доступны операции чтения и записи.
- **Блоки хранения данных** (Value block): доступны дополнительные операции: increment, decrement, transfer и restore. При условии доступа ‘001’ возможны только чтение и декремент, «кошелёк» на такой карте невозможно пополнить. При условии доступа ‘110’ пополнение баланса возможно при предъявлении ключа В.
- **Блок данных производителя** (Manufacturer block): доступ только на чтение без возможности записи, для данного блока невозможно установить другие настройки доступа.
- **Управление ключами** (Key management): в транспортной конфигурации для аутентификации должен использоваться ключ А.

Таблица 4. Условия доступа к блокам данных MIFARE® ID

Биты доступа			**Операция**				**Применение**
C1	**C2**	**C3**	**Чтение**	**Запись**	**Инкремент**	**Декремент, транзакция, восстановление**	
0	0	0	Ключ A|B	Ключ A|B	Ключ A|B	Ключ A|B	Транспортная конфигурация*
0	1	0	Ключ A|B	Нет	Нет	Нет	Блок чтения/записи*
1	0	0	Ключ A|B	Ключ B	Нет	Нет	Блок чтения/записи*
1	1	0	Ключ A|B	Ключ B	Ключ B	Ключ A|B	Блок хранения значения*
0	0	1	Ключ A|B	Нет	Нет	Ключ A|B	Блок хранения значения*
0	1	1	Ключ B	Ключ B	Нет	Нет	Блок чтения/записи*
1	0	1	Ключ B	Нет	Нет	Нет	Блок чтения/записи*
1	1	1	Нет	Нет	Нет	Нет	Блок чтения/записи*

* Если для ключа B в условиях доступа в трейлере сектора стоит возможность чтения, ключ не может использоваться для аутентификации (отмечено серым в таблице 3). Соответственно, если считыватель пройдёт аутентификацию для доступа к любому блоку сектора, в трейлере которого прописаны такие условия доступа, и передаст ключ B, карта откажет в любых операциях с памятью.